UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	)	Civil Action No. 23-cv-9518-PAE

PLAINTIFF SECURITIES AND EXCHANGE COMMISSION'S MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

PRELIMINARY STATEMENT 1

BACKGROUND 3

I. There Are Material Disputes of Fact Regarding SolarWinds' Adherence to the Representations in the Security Statement 3

A. There Are Material Disputes of Fact About Whether Defendants' Access Controls Statements Were Misleading 3

1. There Are Material Disputes About the Access Control Deficiencies Flagged in Internal SolarWinds Documents 4

a. A jury should decide whether Brown's warning that the "Current state of security leaves us in a very vulnerable state for our critical assets" was "hyperbole" 4

b. Defendants' attempts to transform key admissions into aspirational statements should be rejected 6

2. There Are Material Disputes About Access Control Deficiencies Identified in Audits 7

3. There Are Material Disputes About the FedRAMP Assessments 9

4. There Are Material Disputes About SolarWinds' Universal Grant of Local Administrator Rights 10

5. There Are Material Disputes About the Security Problems Flagged by Robert Krajcir 11

B. There Are Material Disputes of Fact About Whether Defendants' Password Policy Statements Were Misleading 12

1. There Are Material Disputes About Failures of Password Policy for Shared Accounts 13

2. There Are Material Disputes About the solarwinds123 Password Incident 14

3. There Are Material Disputes About Other Password Failures 15

C. There Are Material Disputes of Fact About Whether Defendants' Secure Development Lifecycle Statements Were Misleading 17

1. There Are Material Disputes Regarding SDL Implementation 17

2. There Are Material Disputes About Threat Modeling 18

3. There Are Material Disputes About the Orion Improvement Program 20

4. There Are Material Disputes About the Lack of Separation Between the Production and Development Environments 21

D. There Are Material Disputes of Fact About Whether Defendants Made Materially Misleading Statements Regarding Following the NIST Cybersecurity Framework ...22

ARGUMENT 22

I. The Legal Standard for Summary Judgment 22

II. The Legal Standard for the SEC's Fraud Claims 24

III. Genuine Disputes of Material Fact Preclude Summary Judgment Regarding the Falsity of the Security Statement 25

A. Defendants' Arguments are Premised on a Fundamental Misunderstanding of the Law of Summary Judgment 25

B. Defendants Misread Summary Judgment Case Law 27

C. Defendants Are Not Entitled to Summary Judgment Regarding the Falsity of Their Access Controls Statements 28

1. The Court Is Not Required to Credit Defendants' Explanations for SolarWinds' Recurring Access Control Problems 28

2. The Court is Not Required to Credit Defendants'' Explanations for Mr. Krajcir's Presentation on a "Security Gap" 29

D. Defendants Are Not Entitled to Summary Judgment Regarding the Falsity of Their Statements About Password Practices 30

1. The Use of Shared Accounts at SolarWinds 30

2. Defendants' Password Failures 31

3. Defendants' Reliance on the Zimmerman Declaration Is Improper 32

E. Defendants Are Not Entitled to Summary Judgment Regarding the Falsity of Their SDL Statements 34

F. Defendants Are Not Entitled to Summary Judgment Regarding Their Misleading Claim to Follow the NIST Cybersecurity Framework 36

G. The Processes and Procedures Described in the Parties' Joint Statement of Facts Do Not Absolve Defendants of Liability. 38

H. The SEC Has Not Changed Its Theory About Defendants' Misconduct.....40

IV. Defendants Are Not Entitled to Summary Judgment on Materiality.....42

V. Defendants Are Not Entitled to Summary Judgment on Mental State.....46

A. A Jury Should Decide Whether Defendants Acted With Scienter.....46

B. There Are Genuine Disputes of Material Fact as to Whether Defendants Acted With Negligence.....48

VI. SolarWinds' and Brown's Misstatements and Omissions Were Made "In Connection With" the Purchase or Sale of Securities.....48

CONCLUSION.....50

TABLE OF AUTHORITIES

Cases

Aaron v. SEC,
446 U.S. 680 (1980) 24

Africa v. Jianpu Tech. Inc.,
21-CV-1419 (JMF), 2022 WL 4537973 (S.D.N.Y. Sept. 28, 2022) 35

Basic Inc. v. Levinson,
485 U.S. 224 (1988) 43, 49

Caiola v. Citibank, N.A., New York,
295 F.3d 312 (2d Cir. 2002) 25, 39

Capitol Records, LLC v. Escape Media Grp., Inc.,
2014 WL 12698683 (S.D.N.Y. May 28, 2014),
report and recommendation adopted,
2015 WL 1402049 (S.D.N.Y. Mar. 25, 2015) 33, 34

Castellano v. Young & Rubicam, Inc.,
257 F.3d 171 (2d Cir. 2001) 43

Castle Rock Entm't, Inc. v. Carol Publ'g Grp., Inc.,
150 F.3d 132 (2d Cir. 1998) 22, 25

Conklin v. U.S. Immigr. & Customs Enf.,
661 F. Supp. 3d 239 (S.D.N.Y. 2023) 34

Cooper v. Clancy,
2023 WL 7281149 (N.D.N.Y. Nov. 3, 2023) 33

D'Addario v. D'Addario,
75 F.4th 86 (2d Cir. 2023) 49

Davis-Garett v. Urban Outfitters, Inc.,
921 F.3d 30 (2d Cir. 2019) 23

DeKalb Cnty. Pension Fund v. Allergan PLC,
No. 23-117, 2024 WL 677081 (2d Cir. Feb. 20, 2024) 36

Donoghue v. Oaktree Specialty Lending Corp.,
2024 WL 3455292 (S.D.N.Y. June 20, 2024) 2, 23, 26, 27

Dyer v. MacDougall,
201 F.2d 265 (2d Cir. 1952) 26

ECA, Local 134 IBEW Joint Pension Trust of Chicago v. JP Morgan Chase Co.,
553 F.3d 187 (2d Cir. 2009) 35

Eckhart v. Fox News Network, LLC,
2025 WL 786536 (S.D.N.Y. Mar. 12, 2025) 24

Fleming v. Verizon N.Y. Inc.,
2006 WL 2709766 (S.D.N.Y. Sept. 22, 2006) 32

Gillis v. QRX Pharma Ltd.,
197 F. Supp. 3d 557 (S.D.N.Y. 2016) 35, 36

Goldman v. Belden,
754 F.2d 1059 (2d Cir. 1985) 43

Hemming v. Alfin Fragrances, Inc.,
690 F. Supp. 239 (S.D.N.Y. 1988) 50

Howard v. Arconic Inc.,
395 F. Supp. 3d 516 (W.D. Pa. 2019) 50

In re Aluminum Warehousing Antitrust Litig.,
336 F.R.D. 5 (S.D.N.Y. 2020) 41

In re Austl. & N.Z. Banking Grp. Ltd. Sec. Litig.,
No. 08 Civ. 11278 (DLC), 2009 WL 4823923 (S.D.N.Y. Dec. 14, 2009) 35

In re Dana Corp.,
574 F.3d 129 (2d Cir. 2009) 23, 24, 29

In re Equifax Inc. Sec. Litig.,
357 F. Supp. 3d 1189 (N.D. Ga. 2019) 45

In re Glob. Crossing, Ltd. Sec. Litig.,
322 F. Supp. 2d 319 (S.D.N.Y. 2004) 47

In re Heartland Payments Sys., Inc. Sec. Litig.,
2009 WL 4798148 (D.N.J. Dec. 7, 2009) 45

In re Intel Corp. Sec. Litig.,
2019 WL 1427660 (N.D. Cal. Mar. 29, 2019) 45

In re Joint E. & S. Dist. Asbestos Litig.,
52 F.3d 1124 (2d Cir. 1995) 41

In re Marriott Int'l, Inc.,
31 F.4th 898 (4th Cir. 2022) 45

In re Miller Indus., Inc.,
120 F.Supp.2d 1371 (N.D. Ga. 2000) 44

In re Morgan Stanley Info. Fund Sec. Litig.,
592 F.3d 347 (2d Cir. 2010) 31, 37, 39

In re Motel 6 Sec. Litig. v. Thrasher,
161 F. Supp. 2d 227 (S.D.N.Y. 2001) 30

In re SolarWinds Corp.,
595 F. Supp. 3d 573 (W.D. Tex. 2022) 45

Janus Capital Group, Inc. v. First Derivative Traders,
564 U.S. 135 (2011) 47, 48

Kaytor v. Elec. Boat Corp.,
609 F.3d 537 (2d Cir. 2010) 22, 23

Kleinman v. Elan Corp., plc,
706 F.3d 145 (2d Cir. 2013) 37

Lindblom v. Mobile Telecommunications Techs. Corp.,
985 F. Supp. 161 (D.D.C. 1997) 50

Lujan v. Cabana Mgmt., Inc.,
284 F.R.D. 50 (E.D.N.Y. 2012) 34

Macquarie Infrastructure Corp. v. Moab Partners, L.P.,
601 U.S. 257 (2024) 37

Matrixx Initiatives, Inc. v. Siracusano,
563 U.S. 27 (2011) 40

Meyer v. Jinkosolar Holdings Co., Ltd.,
761 F.3d 245 (2d Cir. 2014) ..... passim

Moll v. Telesector Res. Grp., Inc.,
94 F.4th 218 (2d Cir. 2024) 23, 29, 38

NAF Holdings, LLC v. Li & Fung (Trading) Ltd.,
2016 WL 3098842 (S.D.N.Y. June 1, 2016) 37

Novak v. Kasaks,
216 F.3d 300 (2d Cir. 2000) 47

Olkey v. Hyperion 1999 Term Tr., Inc.,
98 F.3d 2 (2d Cir. 1996) 43

P. Stoltz Family P'ship L.P. v. Daum,
355 F.3d 92 (2d Cir. 2004)..... 45

Patterson v. Balsamico,
440 F.3d 104 (2d Cir. 2006)..... 33

Plumber & Steamfitters Local 773 Pension Fund v. Danske Bank A/S,
11 F.4th 90 (2d Cir. 2021) 32, 35

Poller v. Columbia Broad. Sys., Inc.,
368 U.S. 464 (1962)..... 24

Press v. Chem. Inv. Servs. Corp.,
166 F.3d 529 (2d Cir. 1999)..... 46

Reeves v. Sanderson Plumbing Products, Inc.,
530 U.S. 133 (2000)..... 23, 38

Rule v. Brine, Inc.,
85 F.3d 1002 (2d Cir. 1996)..... 24

SEC v. Apuzzo,
689 F.3d 204 (2d Cir. 2012)..... 44

SEC v. Cole,
2015 WL 5737275 (S.D.N.Y. Sept. 19, 2015)..... 48, 49

SEC v. Constantin,
939 F. Supp. 2d 288 (S.D.N.Y. 2013)..... , 48

SEC v. DeFrancesco,
699 F. Supp. 3d 228 (S.D.N.Y. 2023)..... 46

SEC v. Frohling,
851 F.3d 132 (2d Cir. 2016)..... 24

SEC v. Gabelli,
653 F.3d 49 (2d Cir. 2011),
rev'd on other grounds, 568 U.S. 442 (2013)..... 37

SEC v. Ginder,
752 F.3d 569 (2d Cir. 2014)..... 24, 48

SEC v. Mahabub,
343 F. Supp. 3d 1022 (D. Colo. 2018),
aff'd sub nom. SEC v. GenAudio Inc.,
32 F.4th 902 (10th Cir. 2022) 50

SEC v. McNulty,
137 F.3d 732 (2d Cir. 1998) 46

SEC v. Morgan,
2019 WL 2385395 (W.D.N.Y. June 5, 2019) 49

SEC v. Obus,
693 F.3d 276 (2d Cir. 2012) 46

SEC v. Simeo,
2021 WL 4041562 (S.D.N.Y. Sept. 3, 2021) 48

SEC v. SolarWinds Corp.,
741 F. Supp. 3d 37 (S.D.N.Y. 2024) ..... passim

SEC v. StratoComm Corp.,
2 F. Supp. 3d 240 (N.D.N.Y. 2014),
aff'd 652 F. App'x 35 (2d Cir. 2016) 49

SEC v. Terraform Labs Pte. Ltd.,
708 F. Supp. 3d 450 (S.D.N.Y. 2023) 24, 43, 46

SEC v. Univ. Express, Inc.,
475 F. Supp. 2d 412 (S.D.N.Y. 2007),
aff'd sub nom. SEC v. Altomare,
300 F. App'x 70 (2d Cir. 2008) 46, 48

SEC v. Yorkville Advisors, LLC,
305 F. Supp. 3d 486 (S.D.N.Y. 2018) 36

Shenk v. Karmazin,
868 F. Supp. 2d 299 (S.D.N.Y. 2012) 36

St. Pierre v. Dyer,
208 F.3d 394 (2d Cir. 2000) 29

Tieu v. New York City Econ. Dev. Corp.,
717 F. Supp. 3d 305 (S.D.N.Y. 2024) 27

TSC Indus., Inc. v. Northway, Inc.,
426 U.S. 438 (1976) 43

United States v. Litvak,
808 F.3d 160 (2d Cir. 2015) 42

United States v. Naftalin,
441 U.S. 768 (1979) 49

Ventra v. United States,
121 F.Supp.2d 326 (S.D.N.Y. 2000) 32

Statutes

15 U.S.C. § 77q 24

15 U.S.C. § 78j 24

17 C.F.R. § 240.10b-5 ..... 24, 40

Rules

Fed. R. Civ. P. 56 22

Fed. R. Civ. P. 37 32

Plaintiff Securities and Exchange Commission ("SEC") respectfully submits its Memorandum of Law in Opposition to Defendants' Motion for Summary Judgment ("Motion"). [ECF No. 184]. For the reasons set forth below, SolarWinds and Timothy Brown ("Defendants") have failed to show that they are entitled to judgment. The SEC respectfully requests that the Court deny the Motion in its entirety.

PRELIMINARY STATEMENT

The evidence obtained in discovery has confirmed this Court's prior determination, made in the context of Defendants' motion to dismiss, that SolarWinds' contemporaneous documents demonstrate that Defendants' Security Statement contained "flat falsehoods." *SEC v. SolarWinds Corp.*, 741 F. Supp. 3d 37, 82 (S.D.N.Y. 2024) (finding that Defendants' internal records, many of them sent to or authored by Brown, demonstrate fraud if credited). At a minimum, the plain reading of these documents (and the related witness testimony) present material issues of fact for the jury.

Defendants, in an effort to distract the Court from this compelling conclusion, mount a two-prong defense: First, they ask the Court to ignore the contemporaneous documents that show the Security Statement to be false. [Def. 56.1 at 1].[1] Second (and alternatively), they ask the Court to credit new explanations for Defendants' documents that, at times, contradict other witness testimony obtained in discovery. [Def. Br. at 1-2]. Both arguments seek to turn decades of

[1] The SEC's Memorandum of Law in Opposition to Defendants' Motion for Summary Judgment is referred to as "SEC Opp." The SEC's Rule 56.1 Statement of Undisputed Facts is referred to as "SEC 56.1." The SEC's Response and Counter-Statement to Defendants' Statement of Undisputed Material Facts is referred to as the "Response to Def. 56.1." Defendants' Memorandum of Law In Support of Motion for Summary Judgment, ECF 184, is referred to as "Def. Br." Defendants' Rule 56.1 Statement of Undisputed Facts is referred to as "Def. 56.1." The Parties' Joint Statement of Undisputed Facts, ECF 166, is referred to as "JS." The Declaration of Kristen Warden in Opposition to Defendants' Motion for Summary Judgment is referred to as "Warden Decl." The Declaration of Mark Graff in Support of the SEC's Opposition to Defendants' Motion for Summary Judgment is referred to as "Graff Decl."

summary judgment law on its head. At this stage, the Court must resolve ambiguities and conflicts in evidence in favor of the SEC as the non-moving party. *See Castle Rock Entm't, Inc. v. Carol Publ'g Grp., Inc*., 150 F.3d 132, 137 (2d Cir. 1998) (cleaned up). And the Court should reject Defendants' attempts to require the Court to decide whether the newly proposed explanations are credible. *See Donoghue v. Oaktree Specialty Lending Corp.*, 2024 WL 3455292, at *8 (S.D.N.Y. June 20, 2024) (Engelmayer, J.) (juries should evaluate critical testimonial evidence). Indeed, when a defendant resorts to explanations such as disclaiming his own incriminating words as "hyperbole," it only underscores that the Court should allow a jury to evaluate whether those explanations are credible.

Defendants also rely heavily on their contention that SolarWinds "routinely implemented each of the challenged policies," claiming that this fact "dooms" the SEC's case. [Def. Br. at 1]. But simply having policies and procedures in place as to each of the subject areas does not negate the SEC's core allegation that the Security Statement was misleading. Further, by touting their strong cybersecurity practices in the Security Statement, Defendants had a ***legal duty*** to tell the whole truth about the significant cybersecurity problems they were documenting internally to avoid creating a misleading impression to investors. It is axiomatic that "half-truths" will support a claim for securities fraud. Here, the full truth is that despite having some cybersecurity policies and procedures in place, Defendants documented material failures with respect to them.

Given the conflict between the documentary record and the after-the-fact explanations offered by SolarWinds' affiliated witnesses, the proper course is for a jury to sort out these disputed material facts at trial. The Court should reject Defendants' attempts to circumvent the summary judgment standard with their witnesses' newly discovered explanations for documents that on their faces describe SolarWinds' pervasively poor cybersecurity practices.

BACKGROUND

I. There Are Material Disputes of Fact Regarding SolarWinds' Adherence to the Representations in the Security Statement.

The Security Statement claimed that SolarWinds had robust access controls, enforced a password policy, used a Secure Development Lifecycle ("SDL") for software development, and followed the NIST Cybersecurity Framework ("NIST CSF"). The plain language of numerous contemporaneous documents contradicts those representations, as the Court recognized in deciding the motion to dismiss. *See, e.g.*, *SolarWinds Corp.*, 741 F. Supp. 3d at 82 (documents set forth in Amended Complaint support plausible allegations of "sustained public misrepresentations, indeed many amounting to flat falsehoods, in the Security Statement about the adequacy of its access controls."). Now, however, Defendants seek summary judgment on the basis that SolarWinds employees and former employees have provided explanations for those documents during the litigation and that the Court must credit those explanations. Defendants' arguments only serve to highlight the numerous disputed material facts at the core of this litigation.

A. There Are Material Disputes of Fact About Whether Defendants' Access Controls Statements Were Misleading.

The Security Statement represented that SolarWinds employed robust access controls, including utilizing the principle of least privilege and only granting employees a "limited set of default permissions to access company resources." [JS ¶71]. The evidence, however, presents a material dispute of fact about whether Defendants failed to disclose significant access control discrepancies that contradict these representations. As discussed below, SolarWinds' internal analyses reported access control deficiencies throughout the Relevant Period (October 2018 through January 2021). Likewise, internal and external audits following the SUNBURST

incident showed significant deficiencies in access controls. SolarWinds' internal FedRAMP assessments also demonstrated numerous access control deficiencies. Lastly, SolarWinds' policy of granting local administrator access to users poses a conflict with the Security Statement's representations regarding access controls and authentication and authorization. Whether this contradiction rendered the Security Statement's representations misleading presents a quintessential issue of material fact to be decided by a jury.

1. There Are Material Disputes About the Access Control Deficiencies Flagged in Internal SolarWinds Documents.

Numerous internal documents and communications highlight persistent issues with access controls. For example, multiple quarterly risk reviews drafted with input from Tim Brown and shared with SolarWinds' senior management acknowledged "significant deficiencies" in user access management and other problems. [*See, e.g.*, JS ¶177 ("[a]ccess and privilege to critical systems/data is inappropriate" with NIST maturity rating of "1" for "Authentication, Authorization and Identity Management"); ¶¶179, 181-183; SEC 56.1 ¶¶59, 77-92]. Defendants now rely on post-hoc explanations for these and other incriminating documents. [*See* Def. Br. 8-13; *see generally* Def. 56.1 ¶¶ 10-86]. But those explanations just create conflicting explanations for a jury to resolve.

a. A jury should decide whether Brown's warning that the "Current state of security leaves us in a very vulnerable state for our critical assets" was "hyperbole."

Defendants ask this Court to disregard, as "hyperbole," the October 2018 Information Security Risk Review, which was prepared by Brown for SolarWinds' management. That document stated, under the subheading "Risk of Non-Investment," that the "Current state of security leaves us in a very vulnerable state for our critical assets." [JS ¶172; SEC 56.1 ¶¶56-60]. Defendants now claim that this language was "merely hyperbole intended to underscore the

importance of investing in cybersecurity and increase the likelihood his budget request would be granted" and "not intended to convey that SolarWinds was pervasively failing to implement role-based access controls (or any other practices described in the Security Statement)." [Def. 56.1 ¶¶77-79].

As an initial matter, this language appears in multiple documents in 2017 and 2018. [JS¶¶159, 161, 164, 172, 173]. The repetition of this language in multiple presentations over more than a year further undermines the claim this was merely hyperbole. [*Id.*].

In the October 2018 presentation, the language appears with a progress report showing the font color changed to yellow. Defendants claim that "all Mr. Brown meant to convey by yellow font is that improvements had been made since August 2017, but there was still work to be done." [JS ¶172; Def. 56.1 ¶¶82-85].

Undercutting the defense attempts to downplay the document, however, is Brown's admission that this statement was sent to his supervisor, Chief Information Officer Rani Johnson. [JS ¶173; SEC 56.1 ¶¶55-58]. And while Brown now attests in a declaration filed with his motion that the statement was "merely hyperbole," at his deposition Brown testified that he did "n[o]t recall [his] state of mind" when he made the statement. [Def. 56.1 ¶77; SEC 56.1 ¶¶59-61]. Brown also could not recall which tasks had been performed as of October 2018 with respect to this item. [SEC 56.1 ¶62]. This conflict between (a) the plain words of the document, (b) Brown's prior testimony, and (c) his current explanation is more than sufficient to present an issue of material fact that the jury must resolve. [*See also* SEC 56.1 ¶¶19, 55-65, 77-79*;* Response to Def. 56.1 ¶¶ 77-81, 84-86].

b. Defendants' attempts to transform key admissions into aspirational statements should be rejected.

SolarWinds' May and August 2019 Security & Compliance Overviews included a discussion of a program to address enterprise access management and SOX compliance and noted that the "Concept of least privilege not followed as a best practice." [SEC 56.1 ¶¶74-80; JS ¶178]. The documents also flagged the "[u]se of shared accounts throughout internal and external applications." [*Id.*] Attempting to neutralize these incriminating words, Defendants submit a declaration from SolarWinds' then-director of internal audit, Danielle Campbell, who claims that "most of the work for the project had been completed by early 2019." [Response to Def. 56.1 ¶88]. Notably, Ms. Campbell states that she ***does not know*** what was referred to by "Concept of least privilege not followed as a best practice," but nevertheless asserts that it did not refer to any "pervasive" problem that was uncovered as a part of SolarWinds' SOX-related work. [Response to Def. 56.1 ¶90]. Even if a jury were to credit this after-the-fact explanation, this would leave open the question of whether SolarWinds omitted its failures regarding least privilege earlier in the Relevant Period. But at its core, Ms. Campbell's explanation contradicts the plain words of the document and presents a material dispute of fact.

Similarly, SolarWinds' internal NIST scorecard from its August 2019 quarterly security review stated that, "Access and privilege to critical systems/data is inappropriate" and assessed a NIST maturity level of "1" out of 5 for "Authentication, Authorization and Identity Management." [JS ¶177; SEC 56.1 ¶¶81-88]. Defendants now argue, based on a recent declaration from Ms. Johnson, that this simply referred to an ongoing project to migrate from a manual access rights System Access Request Form ("SARF") system to an automatic system, Microsoft Azure Active Directory ("AD"). [*See* Def. Br. at 27-29]. The Security and Compliance reviews, however, stated that access was "inappropriate," not merely that it was in a process of

being transferred to Azure AD. [SEC 56.1 ¶¶88, 254]. Further, Ms. Johnson testified at her deposition that this statement was referring to yet a different upgrade, called Thycotic Secret Server, to manage privileged access credentials in a secret server, thus presenting a material conflict within her own testimony. [SEC 56.1 ¶89]. Putting aside the internal contradictions within Ms. Johnson's accounts, either of her proffered explanation is different than the plain words of the contemporaneous document. Likewise, at his deposition, Brown, who composed the NIST scorecards along with Ms. Johnson, could not recall the basis for the statement that access was "inappropriate" or what "critical systems/data" or "access and privilege" were being referred to in this statement, but he now agrees with Ms. Johnson's declaration. [SEC 56.1 ¶¶90-92]. Again, these are material disputes of fact.

In other examples, SolarWinds' March, May, and October 2020 Quarterly Risk Reviews, which were drafted with input from Brown and shared with Ms. Johnson and Mr. Kim, identified that there were "significant deficiencies in user access management," and acknowledged that "security processes [were] not consistently implemented." [SEC 56.1 ¶¶102-111; JS ¶¶181, 182, 183]. Similar to the August 2019 quarterly security review, Defendants now argue that these statements simply referred to the ongoing process to automate access management through Azure AD. [Def. Br. at 28-29; Def. 56.1 ¶37]. As with the August 2019 quarterly security review, this conflict between the plain language of the document and Defendants' after-the-fact explanation presents a material dispute of fact. [*See also* SEC 56.1 ¶¶15-31, 64-92, 102-111; Response to Def. 56.1 ¶¶30-31, 36-37].

2. There Are Material Disputes About Access Control Deficiencies Identified in Audits.

SolarWinds also identified two control deficiencies for "access provisioning" in its March 2020 (fiscal year 2019) Sarbanes-Oxley ("SOX") audit, and listed Brown as the "control owner"

for those deficient controls. [JS ¶188; SEC 56.1 ¶¶123-131]. To counteract SolarWinds' internal audit findings showing deficiencies in access provisioning from this audit, Defendants rely on Ms. Campbell's declaration, which includes a claimed explanation for treating these deficiencies as control deficiencies rather than significant deficiencies or material weaknesses for purpose of SolarWinds' SOX compliance, and generally minimizes their importance. [*See* Def. 56.1 ¶¶117-124]. But the plain language of the audit found that "password complexity was not enforced" and "logical access rights were not removed in a timely manner for 4 terminated users." [SEC 56.1 ¶¶128, 131]. Whether these deficiencies, along with the other noted problems render the Security Statement materially misleading is an issue of fact for the jury.

Two key audits following the SUNBURST incident also identified several deficiencies in SolarWinds' access controls. First, SolarWinds' internal audit group, with assistance from KPMG, assessed SolarWinds' internal controls over financial reporting through December 31, 2020. The report found that SolarWinds had inadequate authentication controls over certain accounts that had access to financial reporting systems or infrastructure. [SEC 56.1 ¶¶135-147]. And the report found these problems aggregated to a significant deficiency. [SEC 56.1 ¶148].

Second, SolarWinds' external auditors from PricewaterhouseCoopers, LLP ("PwC") aggregated the effect of several control deficiencies in its analysis of SolarWinds' Information Technology General Controls after the SUNBURST incident and concluded that, in the aggregate, the control deficiencies relating to access controls resulted in a significant deficiency. [SEC 56.1 ¶¶149-156]. Thus, PwC's conclusions regarding the severity of SolarWinds' control deficiencies contradict the company's internal assessments of those control deficiencies,

presenting another material issue of fact.[2] [*See also* SEC 56.1 ¶¶ 115-131, 133-156; Response to Def. 56.1 ¶¶39-43, 124].

3. There Are Material Disputes About the FedRAMP Assessments.

Despite SolarWinds' conclusion in its FedRAMP assessments that many of SolarWinds' access controls did not meet the NIST 800-53 standards, Defendants argue that these assessments do not conflict with SolarWinds' representations in the Security Statement regarding the same access controls. [*See* Def. Br. at 29-31]. Although the FedRAMP analysis concerned the FedRAMP standards as evaluated against NIST 800-53 rather than the representations in the Security Statement *per se*, the findings in the FedRAMP analysis nonetheless are relevant to the representations in the Security Statement. For example, the finding that SolarWinds conducted no audit on whether the concept of least privilege was in place directly bears on the representations of the Security Statement. [SEC 56.1 ¶¶94-95; 171]. Put another way, a failure to meet NIST 800-53 does not automatically render the Security Statement false, but a specific finding in the NIST 800-53 analysis that directly contradicts a representation in the Security Statement cannot be dismissed simply because NIST 800-53 is more demanding overall.

Defendants claim that the only relevant control in the FedRAMP assessment (a) concerned the principle of least privilege and (b) only addressed whether an audit had been performed rather than whether the practice was in place. [*See* Def. Br. at 30-31]. This ignores other pertinent controls cited in the FedRAMP assessment, including: "The organization restricts privileged accounts on the information systems to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information]."

[2] Even though these audits were not completed until after the Relevant Period, they are still relevant as they assessed the state of cybersecurity during the Relevant Period and undercut the current Defense explanations that there were no significant problems during the Relevant Period.

[SEC 56.1 ¶94]. The assessment for this was "[w]e have no explicit authorization policy, nor is this documented that I am aware of for the company or individual products." [*Id.*]. There are multiple other examples as well. [SEC 56.1 ¶¶95-99]. These specific findings in the FedRAMP assessments are evidence that create disputes regarding Defendants' claim to adhere to the Security Statement.

Defendants also attempt to minimize the importance of this analysis by questioning the qualifications of the employee who performed the analysis, Kellie Pierce. [*See* Def. Br. at 29-30]. Defendants describe the FedRAMP as a "preliminary review," *id*., but Ms. Pierce consulted with technical experts and submitted versions of the FedRAMP analysis three times to Brown and/or other senior personnel. [JS ¶¶174-176; SEC 56.1 ¶¶ 93-101, 172]. Moreover, Defendants point to no evidence that SolarWinds ever reached a different conclusion as to whether it was satisfying those standards after a later review. In fact, the evidence supports that they did not: an April 2021 "SolarWinds Enterprise Policy and Procedures Documentation Audit – Executive Summary DRAFT," concluded that only "about 40% of the baseline controls within NIST [800-53] were met or partially met within the policies reviewed." [JS ¶157]. [*See also* Response to Def. 56.1 ¶¶45, 47-48, 50-51, 53-57, 60, 63-67, 69].

4. There Are Material Disputes About SolarWinds' Universal Grant of Local Administrator Rights.

Another set of risks that conflict with the representations in the Security Statement regarding access controls comes from SolarWinds' practice of granting ***all*** users local administrator access. Defendants argue that SolarWinds' internal processes prevented users from having administrator access to all system resources, and therefore the representations in the Security Statement regarding role-based access were accurate. [*See* Def. Br. at 11-13, 33]. However, as Brown acknowledged at his deposition, SolarWinds routinely gave employees ***local*** administrative

access to their own devices, such as laptops. [SEC 56.1 ¶67]. These local administrator rights gave employees the ability to install "anything"—***including malware***—on their devices. [SEC 56.1 ¶68]. Brown testified that SolarWinds thus had to rely on other security resources to prevent malware that would be installed on individual users' devices from spreading to the remainder of SolarWinds' network. [SEC 56.1 ¶69]. A jury could reasonably conclude that this practice conflicted with the Security Statement's representations regarding access controls, including the representation that "SolarWinds employees are granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet." [JS ¶71]. That is because granting every employee local administrator rights to their company-issued laptop is not in fact a "limited set of default permissions." [JS ¶71]. Indeed, the December 2018 Security Operations Summary included an action item under "Privilege Access Management (PAM) and Multifactor Authentication" to "Address the use of local administrator access to non-privileged users. Manage, audit, and apply security controls around privileged access." [SEC 56.1 ¶66]. This action item conflicts with SolarWinds' after-the-fact rationalization. [*See also* SEC 56.1 ¶¶17, 42-45, 112-114].

5. There Are Material Disputes About the Security Problems Flagged by Robert Krajcir.

From June 2018 through January 2020, SolarWinds engineer Robert Krajcir repeatedly raised to security personnel, including SolarWinds Senior InfoSec Manager Eric Quitugua, a security gap posed by the lack of authentication of machines logged into the SolarWinds network and the prevalence of local administrator rights, which Mr. Krajcir identified as a risk to spread malware in SolarWinds' network. [SEC 56.1 ¶¶34, 37, 39-41, 49; JS ¶¶166, 168-170, 180]. Among other things, Mr. Krajcir warned that because of the security gap, SolarWinds employees could "compromise [the] entire network by spreading malware," that SolarWinds had "[n]o means to

enforce or monitor what devices connect to our Network," and that SolarWinds needed to manage the "unlimited" use of admin rights. [JS ¶¶166, 168; SEC 56.1 ¶¶40, 43, 45]. In January 2020, Mr. Quitugua forwarded Mr. Krajcir's August 2018 email to Brown, yet it appears that SolarWinds took no additional action as a result, as the same issues remained as late as January 2021. [SEC 56.1 ¶¶49, 54].

Defendants submit a declaration from Mr. Krajcir in which he claims that the issue he identified did not pertain to role-based access controls. Defendants then argue that the issue raised by Mr. Krajcir did not conflict with the Security Statement because its representation about access controls only pertained to role-based access controls. [*See* Def. Br. at 39 n.30; Def. 56.1 ¶¶70-73]. This interpretation need not be credited on summary judgment because a jury could reasonably read the representations regarding the concept of least privilege to apply to any access to "sensitive data," not just the specific processes for granting of role-based access. [*See* JS ¶71 ("Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis.")]. Moreover, the Amended Complaint refers to the Security Statement as a whole, including the representations relating to SolarWinds employees' "limited set of default permissions to access company resources." [JS ¶71; *see also* SEC 56.1 ¶¶ 34-54; Response to Def. 56.1 ¶¶70-72].

B. There Are Material Disputes of Fact About Whether Defendants' Password Policy Statements Were Misleading.

SolarWinds' Security Statement also stated (a) that its "password policy covers all applicable information systems, applications and databases," (b) that it required users be provisioned with unique account IDs and, (c) that it enforced the use of complex passwords. [JS ¶109]. Contradicting these claims, contemporaneous documents show that SolarWinds had numerous failures regarding password parameters and the use of shared account credentials. Like with the

access control issues, Defendants' proffered post-hoc explanations do not neutralize these contemporaneous documents, but instead create disputed issues of material fact that should be tried to a jury.

1. There Are Material Disputes About Failures of Password Policy for Shared Accounts.

For example, Defendants argue that the Security Statement's representation that "[w]e require that authorized users be provisioned with unique account IDs" was true insofar as users on SolarWinds' network were provided with unique account IDs. [*See* Def. Br. at 13]. Defendants argue that the Security Statement's representation regarding unique IDs was limited to the issuance of user IDs for network access, as opposed to shared accounts used within SolarWinds for other purposes. [*See* Def. Br. at 13; Def. 56.1 ¶99]. But Defendants concede that SolarWinds' internal audits found the use of shared "service accounts," which Defendants define as "accounts intended for use by an application, rather than individual users," and attempted to remediate them. [Def. 56.1 ¶¶92-98].[3]

In addition to earlier documented password issues, *see* SEC 56.1 ¶¶31-32, 176-177, 180-183, at least as of May 2019, SolarWinds had an ongoing project to remedy "Use of shared accounts throughout internal and external applications" with an action item to "Work with teams to decommission use of shared accounts." [SEC 56.1 ¶¶178-179]. In response, Defendants rely on Ms. Campbell's declaration, which claims that this appears to have grown out of an earlier project to remedy use of shared accounts from 2017, and that most of the work had been completed by early 2019. [Def. 56.1 ¶¶87-88; *see also* Def. 56.1 ¶¶92-98; Response to Def. 56.1 ¶¶88-90; JS ¶184 (discussing earlier project to address use of shared accounts)]. As with the

[3] The evidence cited in support of SolarWinds' access controls deficiencies in Section I.A., *supra*, is also evidence of SolarWinds' repeated failure to comply with its own password policy.

action item in the project pertaining to least privilege, Ms. Campbell states that she does not know what was meant by "Use of shared accounts throughout internal and external applications," but claims it did not refer to any "pervasive" problem that was uncovered as a part of SolarWinds' SOX-related work. [Response to Def. 56.1 ¶90]. This conflict between the plain words of the document and Ms. Campbell's explanation presents a material dispute of fact.

2. There Are Material Disputes About the solarwinds123 Password Incident.

The Security Statement represented that "[o]ur password best practices enforce the use of complex passwords that include both alpha and numeric characters," and that this practice "covers all applicable information systems." [JS ¶109]. Despite this, in late 2019 the password for the Company's Akamai server, which was publicly available, was "solarwinds123." [JS ¶187; SEC 56.1 ¶¶161-68]. An outside security researcher brought this weak password to SolarWinds' attention, and Brown forwarded it internally, stating:

> With that credential they could upload anything to downloads.solarwinds.com. I have assumed this was our main download site…The point they were making was that they could have corrupted one our downloads. Replacing files or corrupting what was present in our download site. This was managed and resolved quickly but it did take place and a very weak password existed to access that environment.

[SEC 56.1 ¶168].

Now, after the fact, Defendants argue that this incident does not show falsity of the Security Statement's representation that SolarWinds enforces the use of complex passwords as it was one incident and involved a third-party server for which SolarWinds could not enforce use of a complex password through automatic enforcement mechanisms. [Def. Br. at 35-36; Def. 56.1 ¶¶109-116]. Defendants also claim that, "while the security researcher who found the password was concerned that it could be used to distribute malicious software to alter the files SolarWinds made available to customers for download, in fact the password did not have this ability." [Def. 56.1 ¶114]. In support of this statement, Defendants rely upon a declaration from Brown, who

seeks to retract a statement he made in an email about the seriousness of this issue and instead defers to the declaration of a SolarWinds senior manager, Lee Zimmerman.[4] [Def. 56.1 ¶114]. Brown did not raise any such qualification at the time, however. And in his investigative testimony, Mr. Quitugua confirmed that with that password, anyone could upload executable files into this server that was used to distribute SolarWinds software to customers. [SEC 56.1 ¶164]. All Defendants' current post-hoc explanation can do is create issues of fact for a jury to resolve regarding these contradicting explanations. [*See* Response to Def. 56.1 ¶¶109-116; *see also* SEC 56.1 ¶¶ 161-170].

3. There Are Material Disputes About Other Password Failures.

The evidence shows that SolarWinds was aware of flaws in its password policies relating to enforcement of its use of complex passwords over a number of years during the Relevant Period, and that the issues were brought to the attention of senior management. [SEC 56.1 ¶¶29-30, 103, 173-179; Response to Def. 56.1 ¶113; s*ee also, e.g.*, JS ¶¶184-189]. There were also instances where passwords were not correctly stored in an encrypted state, in contravention of the Security Statement. [SEC 56.1 ¶¶180-183]. Determining whether this frequency and/or severity of these reported issues rises to the level of pervasive failures is a matter for a jury.

Likewise, Defendants argue that the Security Statement's representation that "[o]ur password best practices enforce the use of complex passwords" was accurate because the "best practices" did not imply that SolarWinds could enforce the use of complex passwords automatically in all circumstances. [*See* Def. Br. at 13-15, 35; JS ¶109]. But the Security Statement makes no such qualification as to whether SolarWinds would "enforce" its password requirements only when

[4] *See infra* at § III.D.3 regarding why the Court should not consider Mr. Zimmerman's Declaration.

possible to do so through an automatic system. [JS ¶109]. Perfection is not the standard; but whether the failures documented in this record rise to the level of rendering the Security Statement materially misleading is a jury question.

SolarWinds' FY19 SOX audit also found deficiencies relating to passwords and user access. [*See* JS ¶188; *see also* SEC 56.1 ¶¶133, 174-175]. Similar to the access control deficiencies from the same audit, Defendants rely upon a declaration from Ms. Campbell to claim that the password deficiencies were "considered minor" and only involved password age and history requirements that were required by internal policies but not explicitly referred to in the Security Statement. [Def. 56.1 ¶¶117-24]. Whether a failure to follow internal policies for passwords, such as age and history requirements, falls within the Security Statement's representation that SolarWinds follows "password best practices" presents a material issue of fact. [JS ¶109]. Moreover, the FY19 SOX audit also found at least one instance of the password complexity requirement not being enforced, which conflicts with Defendants' representation that both password deficiencies involved age and history requirements but not complexity. [*Compare* SEC 56.1 ¶128 (acknowledging as a control deviation that "password complexity was not enforced"), *with* Def. 56.1 ¶122 ("Both deficiencies concerned systems on which password complexity requirements were enforced, but not password age and history requirements.")]. There were also instances where passwords were not correctly stored in an encrypted state, in contravention of the Security Statement. [SEC 56.1 ¶¶ 180-183]. As with the deficiencies regarding access controls for this audit, whether these deficiencies conflict with the Security Statement's representations, or whether to credit SolarWinds' explanation that the issues were "minor," presents a material issue of fact. [*See also* SEC 56.1 ¶¶ 171-175; Response to Def. 56.1 ¶124].

C. There Are Material Disputes of Fact About Whether Defendants' Secure Development Lifecycle Statements Were Misleading.

There are disputed issues of material fact as to whether the Security Statement contains material misstatements about SolarWinds' SDL practices. The Security Statement claimed that SolarWinds followed a "defined methodology" for developing secure software, with a "secure development lifecycle" and "standard security practices," but, contrary to these claims, documents show that SolarWinds had not yet rolled out its formalized SDL throughout the organization. [JS ¶140; SEC 56.1 ¶¶189-198]. Evidence also shows that the Security Statement was false because SolarWinds did not deploy threat modeling and that the SDL did not include the Orion Improvement Program. [SEC 56.1 ¶¶198-214; Def. Br. at 38-39; Def. 56.1 ¶¶174-181]. The Security Statement also stated that SolarWinds "maintains separate development and production environments," which is a standard security practice, when evidence shows that was not the case in key, long-standing instances. [SEC 56.1 ¶¶215-224]. This evidence presents material issues of fact as to whether the SDL representations were misleading. Defendants' post-hoc explanations just highlight these disputes. [*See also* SEC 56.1 ¶¶ 184-187; Response to Def. 56.1 ¶¶126, 134, 136, 138].

1. There Are Material Disputes Regarding SDL Implementation.

Internal documents, including emails from SolarWinds engineering director Steven Colquitt, stated that SolarWinds was working to adopt the SDL, that adoption rates varied at different locations within the company, and, in the words of Mr. Colquitt that there was "feedback that ***we don't do*** some of the things" included in the Security Statement. [*See* JS ¶¶190-200 (emphasis added); SEC 56.1 ¶¶188-197, 202].

Defendants contend that SolarWinds performed the security testing functions set forth within the SDL, *e.g.*, penetration testing or vulnerability testing, within its engineering teams, and that

the references in the record to adoption of the SDL merely referred to a more formalized process led by Mr. Colquitt that would document these processes with written final security reviews. [*See* Def. Br. at 17-18]. Defendants point to records of components of security practices identified in the Security Statement, such as an email to Mr. Colquitt stating that engineering teams may be performing many of the Security Statement's functions without realizing it, and a declaration from Mr. Colquitt attempting to explain the discrepancies. [*See* Def. Br. at 17-18; Def. 56.1 ¶¶134-138]. This poses an issue of material fact as to whether the specific security practices set forth in the Security Statement were being followed consistently throughout the company. Similarly, to the extent Defendants argue that the reference to a "secure development lifecycle" in the Security Statement refers only to employing security practices such as penetration testing and not to having a formalized SDL process in place, this too poses a material dispute of fact about whether this was misleading. [*See also* SEC 56.1 ¶¶ 188-197; Response to Def. 56.1 ¶¶134, 136, 138].

2. There Are Material Disputes About Threat Modeling.

Defendants argue that SolarWinds' threat modeling practices should not be considered to be part of the SDL representations because the Security Statement does not speak to threat modeling. [*See* Def. Br. at 37-38]. But the evidence shows that threat modeling is an inherent part of an SDL and that SolarWinds engineers considered threat modeling to be part of the SDL and continued to attempt to implement it during the Relevant Period. [*See*, *e.g.*, JS ¶¶191, 195; SEC 56.1 ¶¶185-187; Response to Def. 56.1 ¶¶159-160, 163-166]. These internal SolarWinds communications present, at a minimum, a material issue of fact as to whether threat modeling should be considered to be part of the Security Statement's SDL representations.

Additionally, a July 2019 document prepared by SolarWinds MSP employees Stas Starikevich and Wojciech Pitera, entitled "MSP Products Security Evaluation" stated:

> Design documentation overall is lacking and unstructured for the majority products. In addition, there is no governance in place to help provide consistency. These are crucial for threat modelling & other security activities in [the] SSDLC.[5] This should be covered by architecture, as part of the SSDLC process being formed.

[JS ¶195]. The document also stated: "No threat modelling nor analysis is performed as part of any process (except MSP Backup Engineering). Has multiple pre-requirements to be implemented (external software assets, 3rd party systems list etc)." [JS ¶195]. Similarly, five months later, in December 2019, a document prepared by Mr. Starikevich entitled "MSP Products Security Evaluation MailAssure," stated, "No threat modelling nor analysis is performed as part of any process." [JS ¶196].

In response, Defendants state that SolarWinds' MSP development teams "may not have done formalized threat modeling at the time these documents were prepared in July and December 2019, but they did analyze products for security risks and vulnerabilities." [Def. 56.1 ¶¶167-173]. In the deposition testimony Defendants cite from Mr. Colquitt in support of this claim, however, Mr. Colquitt testified that he "cannot speak to any of the MSP products or MSP engineering" but could only speak to threat analysis more "generally." [Def. 56.1 ¶172 n.182]. Defendants also argue that this presentation should not be considered because the SEC did not depose the documents' authors. [*See* Def. Br. at 32 n.23; Def. 56.1 ¶170]. But the SEC is not required to depose each author of each document, and the document itself constitutes evidence. Moreover, the SEC requested that SolarWinds prepare a 30(b)(6) witness to testify about SolarWinds' knowledge of this document, and that witness did not know the basis for the various statements in the document. [*See* SEC 56.1 ¶¶203-208]. That lack of knowledge should be held

[5] *See* Response to Def. 56.1 ¶163 (explanation that SSDLC refers to how employees used the SDL).

against Defendants, particularly at this stage. [*See also* SEC 56.1 ¶¶198-214; Response to Def. 56.1 ¶¶159-160, 163-166].

3. There Are Material Disputes About the Orion Improvement Program.

With respect to the Orion Improvement Program ("OIP"), Defendants concede that SolarWinds had not implemented an SDL for the OIP but argue that this should not be seen as a misrepresentation because the OIP was supposedly an internal product and not part of the "products" referred to in the Security Statement. [*See* Def. Br. at 38-39; Def. 56.1 ¶¶174-181]. This argument, however, presents an issue of material fact. Whether the OIP, which was an improvement program for one of SolarWinds' "crown jewel" products, Orion, would have been considered by a reasonable investor to be part of the "products" referred to in the Security Statement is an issue of fact to be decided by a jury. Moreover, SolarWinds' engineers communicated at the time that the OIP should be part of the SDL, undercutting Defendants' argument to the contrary. [*See* JS ¶199; SEC 56.1 ¶¶209-210].

Defendants argue that the SolarWinds engineer's statement that the OIP should be included in the SDL arose in the context of SolarWinds learning of the U.S. Trustee Program incident referred to in the Amended Complaint as posing a risk to SolarWinds. [Def. 56.1 ¶¶179-81]. This explanation does not show why summary judgment would be appropriate. SolarWinds engineers contemporaneously stated that they believed the SDL should be "enforced" for the OIP and the SDL should "cover" the OIP, which runs counter to any argument that they are unconnected to the SDL. [*See* JS ¶199]. Further, contrary to Defendants' contention that the engineers were concerned following the U.S. Trustee incident that "an attacker might be trying to ***attack SolarWinds*** through the OIP server," Def. 56.1 ¶180 (emphasis in original), the engineers were explicit in stating that the OIP should be covered by the SDL because of a risk of a threat actor using it to "***tak[e] over all customer installations***." [Response to Def. 56.1 ¶180 (emphasis

added)]. Given SolarWinds engineers' own assessment that the OIP should be covered by SDL, there is at least a material dispute about whether a reasonable investor would have understood that the OIP should have been covered by the SDL. [*See also* SEC 56.1 ¶¶ 209-210; Response to Def. 56.1 ¶¶176-177, 181].

4. There Are Material Disputes About the Lack of Separation Between the Production and Development Environments.

The Security Statement represents that SolarWinds "maintains separate development and production environments," which is a standard security practice. [SEC 56.1 ¶215]. However, internal documents demonstrate that, as of at least November 2019, SolarWinds developers were working inside the production environment, which Chris Day, VP of Global DevOps and Technology Operations, described as a "***significant security and Sox [sic] violation***" and an "ISO violation." [JS ¶186; SEC 56.1 ¶¶216-19 (emphasis added)]. When questioned about this practice by his superiors, a SolarWinds senior product manager responded that it was not something new, but something the team had been doing since the "since the beginning." [SEC 56.1 ¶221]. Additionally, Mr. Quitugua admitted that SolarWinds has experienced security incidents because of errors made when accessing production data and had to document compliance violations because of this poor security practice. [SEC 56.1 ¶ 224].

Brown issued a risk acceptance form for this practice, but SolarWinds continued to leave the issue unresolved long after the due date for it to be fixed in that form. [SEC 56.1 ¶¶222-24]. Whether this incident renders misleading the Security Statement's representation that SolarWinds "maintains separate development and production environments" is an issue of material fact for a jury. [*See also* SEC 56.1 ¶¶ 215-224; Response to Def. 56.1 ¶¶103-108].

D. There Are Material Disputes of Fact About Whether Defendants Made Materially Misleading Statements Regarding Following the NIST Cybersecurity Framework.

Material issues of fact preclude summary judgment regarding Defendants' claim that SolarWinds followed NIST CSF. NIST CSF is a voluntary framework designed to help organizations manage cybersecurity risks. [JS ¶45]. The framework divides cybersecurity activities into five high-level functions: Identify, Protect, Detect, Respond, and Recover. [JS ¶50].

The Security Statement asserted that "SolarWinds follows the NIST Cybersecurity Framework with layered security controls to help identify, prevent, detect, and respond to security incidents." [JS ¶41]. Given the failures and issues described above and in the cited materials, including low scores on NIST scorecards, audits and other similar evaluations, and emails and other messages documenting cybersecurity problems, it was misleading for SolarWinds, as part of the Security Statement's overall effort to portray the Company as having good cybersecurity, to claim to "follow" NIST CSF, JS ¶41, while not disclosing any of these problems or the specific poor scores the company voluntarily gave itself when assessing itself against NIST CSF. [SEC 56.1 ¶ 260; *see* JS ¶¶65-69, 157, 163, 177, 179, 181-83, 197; *see also* SEC 56.1 ¶¶ 55-111, 225-259; Response to Def. 56.1 ¶¶1, 2, 5, 8, 9].

ARGUMENT

I. The Legal Standard for Summary Judgment.

Granting summary judgment is proper "only where there is no genuine issue of material fact to be tried, and the facts as to which there is no such issue warrant the entry of judgment for the moving party as a matter of law." *Kaytor v. Elec. Boat Corp.*, 609 F.3d 537, 545 (2d Cir. 2010); *see also* Fed. R. Civ. P. 56(a). In considering such a motion, "the court must draw all reasonable inferences and resolve all ambiguities in favor of the non-moving party." *Castle Rock Entm't*,

150 F.3d at 137 (cleaned up). That is because "the court's role with respect to such a motion is not to resolve disputed questions of fact but solely to determine whether, as to any material fact, there is a genuine issue to be tried." *Moll v. Telesector Res. Grp., Inc.*, 94 F.4th 218, 227 (2d Cir. 2024) (cleaned up). Thus, "summary judgment should be denied" when issues of material fact could be resolved by a jury for either party. *Davis-Garett v. Urban Outfitters, Inc.*, 921 F.3d 30, 45 (2d Cir. 2019) (citation omitted). In deciding such motions, the court "may not make credibility determinations or weigh the evidence. Credibility determinations, the weighing of the evidence, and the drawing of legitimate inferences from the facts are jury functions, not those of a judge." *Kaytor*, 609 F.3d at 545 (cleaned up).

In conducting its review on summary judgment, a court "may not properly consider the record in piecemeal fashion, trusting innocent explanations for individual strands of evidence; rather, it must 'review all of the evidence in the record.'" *Id.* (quoting *Reeves v. Sanderson Plumbing Products, Inc.*, 530 U.S. 133, 150 (2000)). Indeed, a reviewing court "***must disregard all evidence favorable to the moving party that the jury is not required to believe***." *Moll*, 94 F.4th at 227-228 (quoting *Kaytor*, 609 F.3d at 545) (emphasis in original); *accord Donoghue*, 2024 WL 3455292, at *11. Instead, credit is given to the evidence favoring the party opposing summary judgment and "evidence supporting the moving party that is uncontradicted and unimpeached, at least to the extent that that evidence comes from disinterested witnesses." *In re Dana Corp.*, 574 F.3d 129, 152 (2d Cir. 2009) (quoting *Reeves*, 530 U.S. at 151).

"In sum, summary judgment is proper only when, with all permissible inferences and credibility questions resolved in favor of the party against whom judgment is sought, there can be but one reasonable conclusion as to the verdict." *Moll*, 94 F.4th at 228 (cleaned up). As such, summary judgment is only authorized when there are no genuine issues to be tried because "it is

quite clear what the truth is." *In re Dana Corp.*, 574 F.3d at 151 (quoting *Poller v. Columbia Broad. Sys., Inc.*, 368 U.S. 464, 467 (1962)).

Here, whether to credit the plain words of the document or the after-the-fact (and conflicting) explanations of SolarWinds' employees poses an issue of material fact that should be resolved by a jury. *See Eckhart v. Fox News Network, LLC*, 2025 WL 786536, at *11 (S.D.N.Y. Mar. 12, 2025) ("Assessments of credibility and choices between conflicting versions of events are matters for the jury, not for the court on summary judgment.") (quoting *Rule v. Brine, Inc.*, 85 F.3d 1002, 1012 (2d Cir. 1996)).

II. The Legal Standard for the SEC's Fraud Claims.

Exchange Act Section 10(b) and Rule 10b-5 prohibit any person, in connection with the purchase or sale of any security, from directly or indirectly: (1) employing any device, scheme or artifice to defraud; (2) making an untrue statement of material fact or omitting to state a material fact necessary to make the statements made not misleading; or (3) engaging in any act, practice, or course of business that operates as a fraud or deceit upon any person, in connection with the purchase or sale of a security. *See* 15 U.S.C. § 78j(b); 17 C.F.R. § 240.10b-5. Securities Act Section 17(a) prohibits similar conduct in the offer or sale of any security. *See* 15 U.S.C. § 77q(a). Section 10(b) requires a showing that the defendants acted with scienter. *See Aaron v. SEC*, 446 U.S. 680, 686 n.5, 695 (1980); *SEC v. Frohling*, 851 F.3d 132, 136 (2d Cir. 2016). Section 17(a)(1) requires scienter, but negligence is sufficient to establish liability under Sections 17(a)(2) and (3). *Aaron*, 446 U.S. at 695-97; *SEC v. Ginder*, 752 F.3d 569, 574 (2d Cir. 2014).

"To demonstrate scheme liability, the SEC must prove that defendants: (1) committed a deceptive or manipulative act; (2) in furtherance of the alleged scheme to defraud; (3) with scienter." *SEC v. Terraform Labs Pte. Ltd.*, 708 F. Supp. 3d 450, 478 (S.D.N.Y. 2023) (cleaned up). With respect to misstatement liability, "[e]ven when there is no existing independent duty to

disclose information, once a company speaks on an issue or topic, there is a duty to tell the whole truth." *Meyer v. Jinkosolar Holdings Co., Ltd.*, 761 F.3d 245, 250 (2d Cir. 2014) (citing *Caiola v. Citibank, N.A., New York*, 295 F.3d 312, 331 (2d Cir. 2002) ("[U]pon choosing to speak, one must speak truthfully about material issues.")). "One cannot, for example, disclose in a securities offering (1) a business's peculiar risk of fire, (2) the installation of a comprehensive sprinkler system to reduce fire danger, and omit (3) the fact that the system has been found to be inoperable, without misleading investors." *Id.* at 251.

III. Genuine Disputes of Material Fact Preclude Summary Judgment Regarding the Falsity of the Security Statement.

A. Defendants' Arguments are Premised on a Fundamental Misunderstanding of the Law of Summary Judgment.

To be clear, Defendants are not saying that the documents cited by the SEC are inauthentic, that none of them relate to the Security Statement issues, or that they do not contain the quotes the SEC is using. Instead, Defendants dispute the plain meaning of documents that the Court already recognized were materially inconsistent with the Security Statement. And they do so by introducing post-hoc interpretations from interested witnesses. Whether to credit those post-hoc explanations or the plain meaning of the contemporaneous document is the quintessential jury function. Instead, Defendants claim that "courts do not hesitate to grant summary judgment" when a witness comes in after-the-fact to explain what they think a document really meant. [Def. Br. at 31-32]. This view of summary judgment would upend decades of well-settled law.

Rather, it is well-established that in deciding summary judgment "the court must draw all reasonable inferences and resolve all ambiguities in favor of the non-moving party." *Castle Rock Entm't., Inc*., 150 F.3d at 137 (cleaned up). Under Defendants' theory, the Court must do exactly the opposite. It must fully credit the testimony of Defendants' own witnesses, and it must draw all inferences and resolve all ambiguities in Defendants' favor.

Defendants are wrong. Just last year, in the *Donoghue* case, this Court denied summary judgment to a defendant who offered unrebutted testimony from two witnesses (including himself) on the central material issue to his affirmative defense, even though there was no documentary evidence that could contradict the witness testimony. 2024 WL 3455292, at *8-12. In so doing, this Court recognized that it "must disregard all evidence favorable to the moving party that the jury is not required to believe." *Id.* And although (unlike Defendants here) the *Donoghue* defendant bore the burden of proof as to his affirmative defense, in this case (unlike in *Donoghue*) there is documentary evidence that the jury could rely on to discredit Defendants' witness testimony. Notably, all of the post-hoc explanations for those documents are testimonial explanations (even if presently offered in declaration form). That only reinforces that summary judgment is inappropriate:

> When the critical evidence adduced by a summary judgment movant is testimonial, as here, an additional complication is present. As Learned Hand famously observed, "the carriage, behavior, bearing, manner and appearance of a witness—in short, his 'demeanor'—is a part of the evidence" at trial, and it is "abundantly settled" that a jury should "take into consideration the whole nexus of sense impressions which they get from a witness" in determining whether to credit (or discredit) his testimony.

Id., at *8 (quoting *Dyer v. MacDougall*, 201 F.2d 265, 268 (2d Cir. 1952)). "Thus, notwithstanding that a witness has testified to a fact, a jury might not credit that testimony. When the witness is a party with a personal interest in the lawsuit, a jury may have an additional basis to view such testimony with skepticism." *Id.* (citation omitted).

The witnesses whose testimony Defendants ask the Court to credit are (1) Defendant Timothy Brown, (2) current employees of SolarWinds, (3) former employees of SolarWinds whose actions are implicated by the lawsuit, and (4) a paid expert witness. *See id.*, at *10 (finding witnesses to have interests in the outcome of the case because one was the defendant, and the other witness could see his or his employer's professional reputation harmed by the

outcome of the case). Moreover, in *Donoghue* the defendant did "not come forward with documentary evidence supporting his account." *Id.*, at *11. Here, rather than just an absence of documents, Defendants seek to have the witnesses explain away contemporaneous documents that undermine their current version of events.

B. Defendants Misread Summary Judgment Case Law.

Defendants' attempt to upend the law of summary judgment is based on a misreading of the cases they cite. [*See* Def. Br. at 26, 31-33]. They particularly misapprehend *Tieu v. New York City Econ. Dev. Corp.*, 717 F. Supp. 3d 305, 330 (S.D.N.Y. 2024). *Tieu*, contrary to Defendants' representations, does not stand for the proposition that a court must credit all after-the-fact testimony about a document's meaning if another witness does not contradict it. Indeed, the *Tieu* court recognized the obligation to "draw reasonable inferences in favor of the [non-moving party]." *Id.* However, the document at issue in *Tieu* was a text message that said, "I know you got the news about [the plaintiff]." *Id.* To support her claim of discrimination, the plaintiff asked the court to infer that "news" meant the fact that she was returning from her medical leave, while the author of the text testified that she was referring to the fact that the plaintiff had filed a discrimination lawsuit. *Id.* The court held that it was not required to infer that "news" meant whatever the plaintiff wanted it to mean. *Id.* That is sensible, as the word "news" in the context of that message could refer to nearly any fact about that plaintiff, and there was no reason to think it meant, of all possible facts, the one fact the plaintiff asserted.

The facts of *Tieu* and this case could hardly be more different. Rather than ambiguous terms such as "news," here the SEC is relying on contemporaneous quotes that this Court already found to present at least a *prima facia* conflict with the Security Statement's representations. *See, e.g.*, *SolarWinds Corp.*, 741 F. Supp. 3d at 61 ("Internal assessments also identified access controls as an area needing improvement."), 83 ("The AC further alleges that SolarWinds'

failure to maintain the sound password practices that it touted was documented repeatedly in audits and internal assessments."). Additionally, unlike *Tieu*, in this case there is a voluminous record of Defendants' statements in emails and internal presentations that contradict the Security Statement. So, not only are these statements fundamentally different that than the generic, ambiguous term "news," there are many of them.

In short, when there is a contradiction between the plain language of contemporaneous documents and witness testimony, the law requires that the Court draw the inferences most favorable to the SEC as the non-movant. Thus, when Brown downplays his own prior statements as "hyperbole," there is a material dispute of fact for a jury to resolve. The Court should reject Defendants' attempts to upend this fundamental principle of law.

C. Defendants Are Not Entitled to Summary Judgment Regarding the Falsity of Their Access Controls Statements.

1. The Court Is Not Required to Credit Defendants' Explanations for SolarWinds' Recurring Access Control Problems.

As discussed above, Defendants' post-hoc explanations for the documents describing SolarWinds' deficient access control practices just create material issues of disputed fact. *Supra* Background §I.A. But keeping in mind the legal requirement that all inferences at this stage should be drawn in favor of the SEC as the non-moving party underscores why the Court should deny Defendants' motion. As just a few examples, Defendants are asking the Court, despite the requirement to draw all inferences in favor of the SEC, to find that a jury ***must conclude*** that:

- The statement "Current state of security leaves us in a very vulnerable state for our critical assets" was "hyperbole,"[6] rather than meaning that the then-current state of SolarWinds cybersecurity left it in a very vulnerable state for its critical assets;

[6] Merriam Webster's online dictionary defines hyperbole to mean an "extravagant exaggeration (such as 'mile-high ice-cream cones')." *See https://www.merriam-webster.com/dictionary/hyperbole* (last visited June 3, 2025).

- The statement "[a]ccess and privilege to critical systems / data is inappropriate" means that the company was working on "migrating to Azure AD and rolling out Thycotic," and not that SolarWinds permitted inappropriate levels of access and privilege to some of its critical systems and data;

- The repeated statement (across months) that there were "Significant deficiencies in user access management" refers to a single mistake in conducting a user access review and not that there were longstanding significant deficiencies in user access management.

[*See* Def. 56.1 ¶¶31, 38-43, 77; SEC 56.1 ¶¶19, 55, 59-60, 63, 88, 90, 104-105, 108, 111, 254]. That is a far cry from the facts of *Tieu* and the other cases Defendants cite. Although a jury may, after hearing from the witnesses and viewing the documents, choose to credit Defendants' proffered explanations, there is no legal basis to find that they ***must*** do so.

Indeed, as the Second Circuit held in reversing a grant of summary judgment where witness credibility was at issue, "the fact that their denials were self-serving does not mean that such testimony would not be admissible at trial; the self-serving nature of a witness's statements goes to the statements' weight, not to their admissibility." *In re Dana Corp.*, 574 F.3d at 153. But the Court immediately added that "the weighing of such statements is a matter for the finder of fact at trial, 'not the prerogative of the court on a motion for summary judgment.'" *Id.* (quoting *St. Pierre v. Dyer*, 208 F.3d 394, 405 (2d Cir. 2000)).

2. The Court Is Not Required to Credit Defendants' Explanations for Mr. Krajcir's Presentation on a "Security Gap."

A jury also could reasonably conclude that the issues raised by Mr. Krajcir concerning system access conflict with the Security Statement's representations about access to company resources, thus making this issue inappropriate for summary judgment. As a jury is not required to credit Mr. Krajcir's recent declaration, the Court "must disregard" such evidence in deciding Defendants' Motion. *See Moll*, 94 F.4th at 227-228. Rather, a jury could choose to credit the plain language of Mr. Krajcir's contemporaneous presentation and email, including the stark warning that the security gap could "compromise [the] entire network by spreading malware."

Additionally, Defendants represented to the Court that they viewed Mr. Krajcir's testimony as "irrelevant" and "remarkably unimportant," and opposed the SEC's efforts to take his testimony. ECF No. 147 at 1, 12. But now, in seeking summary judgment, Defendants try to use Mr. Krajcir's one-sided declaration to circumvent the Letters Rogatory process. [*See* Def. Br. at 39 n.30 (citing Def. 56.1 ¶¶70-73)]. The Court should disregard the Krajcir Declaration because allowing Defendants to bolster their position by relying on it is prejudicial to the SEC. The SEC learned for the first time when Defendants filed their Motion for Summary Judgment that Defendants would be using Mr. Krajcir as a witness. *Id.* His declaration gives Defendants an unfair tactical advantage. Although the SEC stands by its representation to the Court that it does not need Mr. Krajcir's deposition to prevail at summary judgment, allowing Defendants to use a one-sided account from him is something else entirely. Put simply, Defendants were able to prepare for summary judgment knowing this tactic gave them the "last word" on an issue for which the SEC has the burden. *See In re Motel 6 Sec. Litig. v. Thrasher*, 161 F. Supp. 2d 227, 244 (S.D.N.Y. 2001) ("[Defendant's] argument ignores the fact that Plaintiffs were not able to depose [expert] regarding his newly asserted opinions.... Plaintiffs clearly would be prejudiced if this Court were to accept the [] Affidavit."). The Court should disregard the Krajcir declaration.

D. Defendants Are Not Entitled to Summary Judgment Regarding the Falsity of Their Statements About Password Practices.

1. The Use of Shared Accounts at SolarWinds

SolarWinds' Security Statement claimed the company had a password policy and provisioned users with unique account IDs. [JS ¶109]. Defendants argue that the Security Statement's representation that "[w]e require that authorized users be provisioned with unique account IDs" was true insofar as users on SolarWinds' network were provided with unique account IDs. [*See* Def. Br. at 13; Def. 56.1 ¶¶92-99; JS ¶¶110-11]. As documented above,

however, several internal reports showed that SolarWinds failed to enforce this policy on a number of occasions. [JS ¶¶184-186, 188; SEC 56.1 ¶¶31-32, 176-183]. Defendants thus fail to show that summary judgment is appropriate.

Even if the statement were held to be literally true, a jury could still find the statement to be misleading by omitting that users were also permitted to use shared IDs in certain instances. *See, e.g.*, *In re Morgan Stanley Info. Fund Sec. Litig.*, 592 F.3d 347, 366 (2d Cir. 2010) ("The literal truth of an isolated statement is insufficient; the proper inquiry requires an examination of Defendants' representations, taken together and in context.…a disclosure about a particular topic, whether voluntary or required, …must be complete and accurate.") (cleaned up). Such an analysis is a matter of jury deliberation, not summary judgment.

2. Defendants' Password Failures

The Security Statement also claimed to enforce the use of complex passwords. [JS ¶109]. That representation is contradicted by multiple internal assessments and audit findings that SolarWinds failed to enforce these policies, and by the incident involving the weak password "solarwinds123" for a download server. [SEC 56.1 ¶¶161-183 *see, e.g.*, JS ¶¶184-89].

Defendants argue their representation that SolarWinds would "enforce" the use of complex passwords should be read as limited to instances where it was possible to enforce the complex passwords automatically. [*See* Def. Br. at 35-36; Def. 56.1 ¶¶111-112]. But the Security Statement makes no such qualification as to whether SolarWinds would "enforce" its password requirements automatically or in some other way. These incidents thus present a material issue of fact as to whether SolarWinds enforced the use of complex passwords.

Regarding the November 2019 use of the "solarwinds123" password, Defendants now claim that the weak password posed no real risk. [*See* Def. Br. at 35-36; Def. 56.1 ¶¶109-116]. Contrary to Defendants' arguments (based on after-the-fact reasoning from an undisclosed

witness), SolarWinds' contemporaneous emails documented the seriousness of the incident. [JS ¶¶187, 189; SEC 56.1 ¶¶167-68]. Defendants argue that this incident did not represent a "systemic" problem. [*See* Def. Br. at 36]. But a jury could reasonably conclude that, if SolarWinds had a system to enforce use of complex passwords for "all applicable information systems," JS ¶109, such an incident would not have been possible. *See, e.g.*, *Plumber & Steamfitters Local 773 Pension Fund v. Danske Bank A/S*, 11 F.4th 90, 103 (2d Cir. 2021) ("[a]ssertions of satisfactory regulatory compliance can be materially misleading if the descriptions of compliance efforts are detailed and specific.") (cleaned up)); *Meyer*, 761 F.3d at 251 (although perfect compliance "may often be unobtainable," the specific statements were misleading because they hid that specific compliance procedures "were then failing to prevent substantial violations.").

3. Defendants' Reliance on the Zimmerman Declaration Is Improper.

The Court should strike or disregard Defendants' eleventh-hour declaration from senior manager Lee Zimmerman, ECF No. 179. Defendants did not identify him in their initial disclosures or any supplement thereto. [Warden Decl. ¶¶7-8]. Nor was Mr. Zimmerman mentioned in any deposition. [Warden Decl. ¶9]. Yet now, six months after the close of fact discovery, Defendants rely on Mr. Zimmerman's declaration alone to support their claim that "Mr. Graff and the SEC greatly overstate the 'magnitude' of [the solarwinds123] incident." [Def. Br. at 36 n.27 (citing Def. 56.1 ¶¶114-16)]. This is improper.

Federal Rule of Civil Procedure 37(c) prohibits a party from using information it failed to disclose in discovery absent substantial justification. *See* Fed. R. Civ. P. 37(c); *Fleming v. Verizon N.Y. Inc.*, 2006 WL 2709766, at *7-8 (S.D.N.Y. Sept. 22, 2006). The rule's purpose "is to prevent the practice of 'sandbagging' an adversary with new evidence." *Ventra v. United States*, 121 F.Supp.2d 326, 332 (S.D.N.Y. 2000) (quotation omitted). Courts apply a four-part

test when deciding to exclude a witness: "(1) the party's explanation for the failure to comply with the disclosure requirement; (2) the importance of the testimony of the precluded witness; (3) the prejudice suffered by the opposing party as a result of having to prepare to meet the new testimony; and (4) the possibility of a continuance." *Patterson v. Balsamico*, 440 F.3d 104, 117 (2d Cir. 2006) (cleaned up).

First, Defendants have no reasonable excuse for their failure to disclose Mr. Zimmerman. The SEC discussed the solarwinds123 incident in its initial complaint, and Defendants have long been on notice that the SEC would make use of it. Defendants' use of catchall phrases in their disclosures such as "[a]ny individuals identified during the course of discovery" or "[i]ndividuals identified in the documents below" does not comply with Rules 26(a) or (e). *See, e.g.*, *Cooper v. Clancy*, 2023 WL 7281149, at *2 n.4 (N.D.N.Y. Nov. 3, 2023) (rejecting argument that "[all] individuals identified in the pleadings and discovery responses by the parties in this litigation" satisfied Rules 26(a) or (e)) (brackets in original).

Second, although the SEC could easily defeat Defendants' motion even if the Court considered the Zimmerman Declaration, it is the sole support for their argument that the SEC overstates the importance of the solarwinds123 password incident—Mr. Zimmerman was not even mentioned in the report of the defense expert regarding this incident. [SEC 56.1 ¶ 170].

Third, the SEC is prejudiced by this new testimony, which Defendants introduced for the first time on summary judgment. Courts have not hesitated to find so where, as here, discovery closed without an opportunity to depose the previously undisclosed declarant. *Conklin v. U.S. Immigr. & Customs Enf.*, 661 F. Supp. 3d 239, 258 (S.D.N.Y. 2023) (substantial prejudice to movant given lack of opportunity to depose declarants); *Capitol Records, LLC v. Escape Media Grp.,*

Inc., 2014 WL 12698683, at *10 (S.D.N.Y. May 28, 2014), report and recommendation adopted, 2015 WL 1402049, at *27-*29 (S.D.N.Y. Mar. 25, 2015) (same).

Finally, granting a continuance to take Mr. Zimmerman's deposition at this late stage, rather than striking his declaration on this motion, would be inefficient, prejudicial, and "would essentially reward [Defendants] for [their] violations of Rule 26" by delaying resolution of this matter even further. *Conklin*, 661 F. Supp. 3d at 258; *see also Lujan v. Cabana Mgmt., Inc.*, 284 F.R.D. 50, 75 (E.D.N.Y. 2012) (continuance—even without pending trial date—would require reopening discovery and delay resolution of fully-briefed motion). The Court has noted that it does not want delays in this case. As such, the Court should strike Mr. Zimmerman's declaration. *See Capitol Records, LLC*, 2014 WL 12698683, at *11 (striking undisclosed witness's affidavit from summary judgment briefing).

E. Defendants Are Not Entitled to Summary Judgment Regarding the Falsity of Their SDL Statements.

With respect to SolarWinds' SDL representations, as set forth above, material issues of fact exist regarding SolarWinds' SDL implementation, inclusion of threat modeling, inclusion of the OIP, and separation of production and development environments. Defendants fail to show that summary judgment is appropriate for any of these issues.

With respect to SDL implementation, Defendants rely upon internal records of internal security testing having been done for certain projects and a declaration from Mr. Colquitt. [*See* Def. Br. at 17-18; Def. 56.1 ¶¶131-138, 143-149]. As set forth above, at most these explanations present an issue of fact as to whether SolarWinds implemented these practices throughout the company during the Relevant Period. [*See* Background § I.C.1, *supra*; JS ¶190].

Defendants argue that promising to follow an SDL does not entail a promise to follow threat modeling because the words "threat modeling" do not appear in the Security Statement. [Def. Br.

at 37-38]. The cases Defendants cite in support, however, are inapplicable because they deal with statements about following "best practices" or "internally recognized standards," but do not an industry-defined methodology like the SDL practices involved here. the specific representations regarding the SDL practices involved here, or any defined methodology similar to the SDL.[7] Moreover, leading industry authorities such as Microsoft and OWASP defined SDL to include threat modeling during the Relevant Period. [SEC 56.1 ¶¶185-187]. At minimum, these industry authorities pose material issues of fact as to whether a reader would reasonably understand the Security Statement's SDL representations to include threat modeling. Further, this dispute is highlighted by SolarWinds' contemporaneous documents showing that SolarWinds employees believed that threat modeling should have been included, which supports a finding of falsity. *See, e.g.*, *Gillis v. QRX Pharma Ltd.*, 197 F. Supp. 3d 557, 597 (S.D.N.Y. 2016) ("contrary facts" or "facts from which it can be inferred that defendants disbelieved what they were saying" would support falsity claim). [*See also* Background § I.C.2, *supra*; JS ¶¶191, 195-96, 199].

Defendants also argue that the Security Statement's reference to having an SDL for "our products" excludes the OIP, which it argues was an internal program not sold to customers. [Def. Br. at 38-39]. In the cases Defendants cite, however, the claimed term was not in the statement at all, whereas here, at a minimum, there is a material dispute about whether the OIP would be

[7] *See Plumber & Steamfitters*, 11 F.4th at 103 ("general declarations" about following banking laws not actionable when "almost every bank makes these statements") (cleaned up); *ECA, Local 134 IBEW Joint Pension Trust of Chicago v. JP Morgan Chase Co.*, 553 F.3d 187, 206 (2d Cir. 2009) (statement that bank "set the standard for best practices in risk management techniques" too general to support liability when "almost every investment bank makes these statements") (cleaned up); *Africa v. Jianpu Tech. Inc.*, 21-CV-1419 (JMF), 2022 WL 4537973, at *9 (S.D.N.Y. Sept. 28, 2022) (stated goal to "lead the initiative of introducing and promoting higher industry standards and best practices" was puffery); *In re Austl. & N.Z. Banking Grp. Ltd. Sec. Litig.*, No. 08 Civ. 11278 (DLC), 2009 WL 4823923, at *11 (S.D.N.Y. Dec. 14, 2009) (statements such as bank "recogni[zing] the importance of effective risk management to its business success" were too general to be actionable).

implicitly included in the Security Statement's representations regarding use of the SDL for SolarWinds' "products."[8] SolarWinds employees also stated at the time that they believed that the OIP should have been included in the SDL. [*See* Background § I.C.3, *supra*; JS ¶199].

Likewise, with respect to the Security Statement's representation that "SolarWinds maintains separate development and production environments," *see* SEC 56.1 ¶ 215, evidence shows SolarWinds having violated this policy in an incident drawing the attention of the chief information officer and Brown. [*See* Background § I.C.4, *supra*; JS ¶186; SEC 56.1 ¶¶215-224]. Defendants argue that SolarWinds had a practice to maintain separate environments and that this incident was isolated in nature. [Def. 56.1 ¶¶100-108]. Whether this incident made the Security Statement's representation misleading presents yet another dispute of material fact.

F. Defendants Are Not Entitled to Summary Judgment Regarding Their Misleading Claim to Follow the NIST Cybersecurity Framework.

In their brief, Defendants seek to deflect from SolarWinds' numerous cybersecurity failures by arguing that the statement that SolarWinds "follows" the voluntary NIST CSF was true insofar as it used the self-assessment framework, and that it was not required to apply any particular controls or receive any particular scores to do so. [*See* Def. Br. at 6-8]. Defendants even say that it was "irrelevant" whether SolarWinds received persistently poor scores on its internal evaluations. [*See id*. at 8]. But, as the SEC has maintained since the inception of this

[8] *See DeKalb Cnty. Pension Fund v. Allergan PLC*, No. 23-117, 2024 WL 677081, at *3 (2d Cir. Feb. 20, 2024) (statements on incidence of breast cancer for implants as a whole did not speak to difference in incidence of breast cancer for textured vs. smooth implants); *SEC v. Yorkville Advisors, LLC*, 305 F. Supp. 3d 486, 533 (S.D.N.Y. 2018) (whether mentioning of collateral for various companies implied cross-collaterization when report does not mention cross-collateralization); *Gillis*, 197 F. Supp. 3d at 597 (statement about likelihood of regulatory approval of drug not impugned when undisclosed facts did not bear on overall likelihood of approval); *Shenk v. Karmazin*, 868 F. Supp. 2d 299, 306-07 (S.D.N.Y. 2012) (representation about specific subscription packages remaining available after merger of satellite radio companies did not contradict price increase for other packages).

case, the issue is not whether the statement that SolarWinds "follows" NIST CSF is literally true, but whether it is materially misleading to make that statement while omitting its persistently low scores reflecting its cybersecurity problems and failures or any mention of those failures themselves. [*See* AC ¶¶76, 91].

Courts in this Circuit have rejected similar claims that a statement's literal truth can override an overall misleading impression from a defendant's statements. *See, e.g.*, *Morgan Stanley*, 592 F.3d at 366 ("The literal truth of an isolated statement is insufficient; the proper inquiry requires an examination of Defendants' representations, taken together and in context.…A disclosure about a particular topic, whether voluntary or required, …must be complete and accurate.") (cleaned up); *Kleinman v. Elan Corp., plc*, 706 F.3d 145, 153 (2d Cir. 2013) ("veracity of a statement or omission is measured not by its literal truth, but by its ability to accurately inform rather than mislead prospective buyers") (quotation omitted); *SEC v. Gabelli*, 653 F.3d 49, 57 (2d Cir. 2011) ("so-called 'half-truths'—literally true statements that create a materially misleading impression—will support claims for securities fraud") (citation omitted), *rev'd on other grounds*, 568 U.S. 442 (2013); *see also Macquarie Infrastructure Corp. v. Moab Partners, L.P.*, 601 U.S. 257, 264 (2024) (misleading for child to tell his parents that he had dessert but omit that "dessert" was an entire cake).

Just as it would be misleading for a child to tell his parents that he had dessert but omit that "dessert" was an entire cake, *see Macquarie*, 601 U.S. at 264, here a jury could reasonably conclude that it was misleading for SolarWinds to state that it "follows" the NIST CSF without mentioning either that it gave itself pervasively low scores in important NIST categories, including access controls, or anything about the other problems discussed above. This poses an issue of material fact requiring jury decision. *See NAF Holdings, LLC v. Li & Fung (Trading)*

Ltd., 2016 WL 3098842, at *9 (S.D.N.Y. June 1, 2016) (Engelmayer, J.) (denying summary judgment where emails could favor either party's position "depending on disputed inferences and, potentially, witness credibility."). A jury is not required to credit Defendants' after-the-fact statements in evaluating the plain language of Defendants' own documents. And on summary judgment, the Court "must disregard all evidence favorable to the moving party that the jury is not required to believe." *Moll*, 94 F.4th at 227-228 (quoting *Reeves*, 530 U.S. at 151). This holds true not just for the specific examples discussed in this memorandum, but for each instance in which Defendants seek to explain away incriminating contemporaneous documents with post-hoc rationalization. [*See* Response to Def. 56.1 ¶¶18, 30-31, 39-43, 50, 55-56, 60, 64-65, 71-72, 77-79, 81, 86, 89-90, 104-105, 107-108, 124, 126, 134, 136, 138, 142, 159, 163-166, 180-181].

G. The Processes and Procedures Described in the Parties' Joint Statement of Facts Do Not Absolve Defendants of Liability.

Defendants lean heavily on the processes and procedures described in the Parties' Joint Statement of Undisputed Facts (ECF No. 166).[9] [*See* Def. Br. at 22-25]. They contend that, for instance, because they "routinely" used their "SARF process" then *ipso facto* the Security Statement was not misleading. [*See id*. at 23]. Defendants, however, misapprehend the nature of the allegations against them and the law in making these assertions. Since the beginning of this case, the SEC has maintained that it is SolarWinds' overall cybersecurity failings that render the Security Statement materially misleading. [*See, e.g.,* AC ¶232].

[9] Ironically, Defendants materially misstate the nature of the Joint Statement of Undisputed Facts by incorrectly inserting the word "Material" into its title when referring to the document. [Def. Br. at 23]. Not only does "Material" not appear in the document's title, but the document also contains a footnote stating, "The SEC wishes to note that, in agreeing that a particular fact is undisputed for purposes of this joint statement, a party is not conceding that such fact is relevant ***or material*** for purposes of summary judgment…." (ECF No. 166 at 1, n.1) (emphasis added).

So even though it is undisputed that SolarWinds had a SARF process that it routinely used to grant employees access to their systems, that does not automatically mean Defendants did not mislead the investing public about the overall strength and effectiveness of their cybersecurity practices. There is evidence describing serious flaws with the company's access controls, user authentication, and passwords. Even if SolarWinds had no independent duty to disclose information about their cybersecurity practices, once the company put out a detailed statement touting those practices as robust, "there is a duty to tell the whole truth." *Meyer*, 761 F.3d at 250 (citing *Caiola*, 295 F.3d at 331). "The literal truth of an isolated statement is insufficient; the proper inquiry requires an examination of defendants' representations, taken together and in context." *Id.* at 250-51 (quoting *Morgan Stanley*, 592 F.3d at 366).

The Second Circuit's decision in *Meyer* is instructive. The statement at issue discussed the defendant's "pollution abatement equipment and its provision of monitoring environmental teams on duty 24 hours a day." *Id.* at 251. The statement disclosed that the defendant stored "dangerous chemicals and wastes," and that it was subject to Chinese regulations regarding the same. *Id.* The statement also "informed investors that compliance with such regulations is costly and that non-compliance may lead to bad publicity, fines, and even a suspension of the business." *Id.* The Second Circuit recognized that all these statements "may be technically true" and that, as investors would know, "these descriptions did not guarantee 100% compliance 100% of the time." *Id.* However, the Court held, "investors would be misled by a statement such as that quoted above if in fact the equipment and 24–hour team were then failing to prevent substantial violations of the Chinese regulations." *Id.* Despite the company's warning of possible risks, its "failure to disclose then-ongoing and serious pollution violations would cause a reasonable investor to make an overly optimistic assessment of the risk." *Id.*

Thus, to prevail on summary judgment, Defendants must do more than show they had a process for provisioning access, or a password policy, or that they had a software development lifecycle process that they mostly attempted to follow. Instead, they must prove that the internally documented problems and lapses in these policies were so insignificant that they had no duty to disclose them to make the Security Statement's representations "in the light of the circumstances under which they were made, not misleading." *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 44 (2011) (quoting 17 C.F.R. § 240.10b-5(b)). On this mixed record, Defendants cannot prove that it is undisputed that their Security Statement was not misleading.

H. The SEC Has Not Changed Its Theory About Defendants' Misconduct.

As with many of Defendants' arguments, their contention that the SEC has a "new theory" to avoid summary judgment is premised on asking the Court to simply adopt their view of the facts in deciding Defendants' motion. [Def. Br. at 33-37]. Defendants contend that the SEC's theory in the Amended Complaint was that SolarWinds had "pervasive" and "systemic" cybersecurity failures, but now it is instead premising its theory of liability on "isolated failures." [*Id.* at 33-34]. Yet, Defendants' characterization is belied by the facts discussed above and in the SEC's Response and Counter-Statement to Defendants' 56.1 Statement, which describe pervasive and systemic cybersecurity failures. For example, Brown's August 2017 statement that the "Current state of security leaves us in a very vulnerable state for our critical assets. A compromise of these assets would damage our reputation and [impact us] financially," was repeated multiple times in 2017 and 2018. [JS ¶¶159, 161, 164, 172, 173; SEC 56.1 ¶¶55-63]. That is not describing an "isolated" failure but rather systemic issues regarding "critical assets." Similarly, the repeated statements in 2020 Quarterly Risk Reviews regarding "significant deficiencies in user access management," are best understood, at least at this stage, as not describing a single isolated incident but rather multiple deficiencies across several months. [JS ¶¶181-183; SEC 56.1 ¶¶102-

111]. More importantly at this juncture, whether something is isolated or systemic is itself a question for the jury.

Thus, Defendants' arguments about factual allegations and legal theories not raised in the Amended Complaint is without merit. [*See* Def. Br. at 33].[10] The factual allegations the SEC raises in opposition to summary judgment concern the same Security Statement and many of the same documents set forth in the Amended Complaint. Likewise, the legal theory remains unchanged: SolarWinds' Security Statement was misleading as to material facts regarding its cybersecurity posture.

Further, as explained in the SEC's opposition to the challenge to Mr. Graff's testimony, filed today, Defendants' attempts to challenge Mr. Graff's conclusion that certain cybersecurity failures at SolarWinds were of such magnitude that they were indicative of "systemic" problems is inappropriate in the context of a *Daubert* motion. *See In re Aluminum Warehousing Antitrust Litig.*, 336 F.R.D. 5, 34 (S.D.N.Y. 2020) (Engelmayer, J.) (a defendant's "critique, although packaged in *Daubert* terms, is in substance a disagreement with [the expert's] conclusions."). Their argument is even less appropriate for resolution in a summary judgment motion. *See In re Joint E. & S. Dist. Asbestos Litig.*, 52 F.3d 1124, 1135 (2d Cir. 1995) ("Trial courts should not arrogate the jury's role in evaluating the evidence and the credibility of expert witnesses by simply choosing sides in the battle of the experts.") (cleaned up).

Finally, Defendants are incorrect in their semantic argument over the meaning of words such as "systemic" and "pervasive." [Def. Br. at 34-37]. Defendants assert that "those terms denote ***frequent*** and ***widespread*** failures." [Def. Br. at 35 (emphasis in original)]. However, Defendants

[10] Indeed, Defendants contradict themselves by also complaining that the SEC is still relying on the same documents quoted in the Amended Complaint. [Def. Br. at 25-26].

falsely equate "systemic" problems with "frequent" problems. An issue need not occur frequently for it to be "systemic." As Mr. Graff explained in his report, based on the fundamental cybersecurity principle "defense-in-depth," a system should be set up in a way to "apply multiple security layers to ensure that vulnerabilities not remediated by one countermeasure are addressed by another." [Ex. 1 to Graff Decl. [Graff Rep.] ¶35.a]. In other words, the fact that one person's actions can create such substantial security risks without checks and balances in place is, in and of itself, a systemic issue. Rather than an individual failure, the lack of appropriate controls is a systemic weakness.[11] For example, if a trader at a brokerage house can make a multi-billon dollar unauthorized trade, it could represent systemic control issues, even if there is not another unauthorized trade. Similarly, the fact that something is done routinely does not mean there is not a systemic failure to do it. Consider an attorney who, 90% of the time properly deposits his clients' funds in a trust account, but 10% of the time misappropriates their funds to pay his gambling debts. The attorney both routinely makes deposits to the trust account and has a systemic and pervasive failure to properly handle client funds. In any event, such fact-bound disputes should be resolved by a jury.

IV. Defendants Are Not Entitled to Summary Judgment on Materiality.

"Determination of materiality under the securities laws is a mixed question of law and fact that the Supreme Court has identified as especially well suited for jury determination." *United States v. Litvak*, 808 F.3d 160, 175 (2d Cir. 2015) (quotation omitted); *see also Terraform*, 708 F. Supp. 3d at 478-79 (same) (quoting *Litvak*). The antifraud provisions' materiality element is

[11] Conversely, just because an issue occurs frequently does not necessarily mean that it is a systemic issue. For example, if a cybersecurity company's threat detection tool frequently generates alerts that later turn out to be false positives, this might suggest a systemic issue. However, these false positives are a known, controlled trade-off: a conservative design choice aimed at minimizing false negatives (missed attacks). So even though the issue (false positives) occurs frequently, it doesn't reflect a systemic breakdown.

satisfied if there is "a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available." *Basic Inc. v. Levinson*, 485 U.S. 224, 231-32 (1988) (quoting *TSC Indus., Inc. v. Northway, Inc.*, 426 U.S. 438, 449 (1976)).

The determination of materiality requires delicate assessments of the inferences a "reasonable shareholder" would draw from a given set of facts and the significance of those inferences, and these assessments are peculiarly ones for the trier of fact. "Summary judgment may not be granted on the ground that alleged omissions are immaterial 'unless they are so obviously unimportant to a reasonable investor that reasonable minds could not differ on the question of their importance.'" *Castellano v. Young & Rubicam, Inc.*, 257 F.3d 171, 180 (2d Cir. 2001) (quoting *Goldman v. Belden*, 754 F.2d 1059, 1067 (2d Cir. 1985)); *see also Terraform*, 708 F. Supp. 3d at 482 ("Whether to credit the SEC's interpretation or defendants' interpretation of the statements at issue, or whether any distinction between those interpretations would have been material to a reasonable investor, is a question for a jury, not for the Court.").

As the Court held in its decision regarding Defendants' motion to dismiss, as to materiality, the Court should analyze the misrepresentations in the Security Statement as:

> collectively bearing on the Statement's central thesis: that the cybersecurity practices of SolarWinds, a software vendor whose public and private customers expected its products to be reliably airtight against cybersecurity intrusions, were strong. A holistic assessment follows from the precept that the investing public evaluates the information available to it, including that provided by the issuer, 'as a whole,' not in pointillistic fashion.

SolarWinds Corp., 741 F. Supp. 3d at 79 (quoting *Olkey v. Hyperion 1999 Term Tr., Inc.*, 98 F.3d 2, 5 (2d Cir. 1996)).

Defendants' arguments against materiality fail in light of these standards. First, Defendants argue that the two stock analysts who were deposed in discovery "never looked at the Security

Statement before this lawsuit or otherwise inquired about the details of SolarWinds' cybersecurity program during the Relevant Period—because investors never asked about such matters." [Def. Br. at 39]. Whether these analysts looked at the Security Statement during the Relevant Period is not relevant in this suit because the SEC, unlike a private litigant, does not need to prove reliance. *See SEC v. Apuzzo*, 689 F.3d 204, 213 (2d Cir. 2012) ("Thus, while a plaintiff must prove reliance (a concept closely akin to causation) in a private securities fraud suit, there is no such requirement in an SEC enforcement action.") (cleaned up). Similarly, Defendants' dependence on *In re Miller Indus, Inc.*, 120 F.Supp.2d 1371, 1380-81 (N.D. Ga. 2000), for the proposition that the Court should find a lack of materiality when the "consistent practice of the analyst community was to disregard" a certain type of information (in that case, value of chassis sales), is inapposite. Here, unlike *Miller*, analysts have testified that they would find it important in determining whether to recommend that investors purchase SolarWinds stock to know whether SolarWinds' claimed cybersecurity practices regarding access controls, password policies, and SDL were followed. [*See* SEC 56.1 ¶¶266-294].

Next, Defendants argue that the Security Statement was only "a general description of a cybersecurity program on a website," and disclosing the discrepancies would "bury the shareholders in an avalanche of trivial information" insofar as the documents only identified "occasional problems to address or improvements to make." [Def. Br. at 40-41]. First, as discussed above, the information was not trivial. Even SolarWinds' CIO, Ms. Johnson, recognized these issues could affect SolarWinds IPO valuation. [SEC 56.1 ¶¶263-265]. Second, if Defendants found their violations of the Security Statement so numerous that disclosing them would pose that much of a burden, they could instead modify, qualify, or retract the Security Statement. But it cannot be the case that a defendant can be allowed to make a materially false

statement because correcting it would involve too many corrective disclosures. Thus, the overall impact of all of the falsities outlined above on a reasonable investor is a matter for jury decision.

Lastly, Defendants argue that their risk disclosures about possible cybersecurity incidents make the statements in the Security Statement immaterial. [*See* Def. Br. at 41-42]. To the contrary, SolarWinds' risk disclosure warned of a potential loss of business or reputational damage as the result of a cybersecurity incident, which illustrated the importance, and thus materiality, of cybersecurity controls to SolarWinds. [*See* SEC 56.1 ¶¶158-159]. Further, a forward-looking risk disclosure does not insulate defendants from misstatement of present facts regarding their cybersecurity practices. *See, e.g.*, *Meyer*, 761 F.3d at 251 ("A generic warning of a risk will not suffice when undisclosed facts on the ground would substantially affect a reasonable investor's calculations of probability."); *see also P. Stoltz Family P'ship L.P. v. Daum*, 355 F.3d 92, 96-97 (2d Cir. 2004) ("misrepresentation of present or historical facts cannot be cured by cautionary language.").[12] [*See also* SEC 56.1 ¶¶ 261-294].

[12] Accordingly, the cases cited by Defendants are inapposite. They involve claims premised on liability due to the fact of a breach rather than representations about the quality of security programs. *See In re Marriott Int'l, Inc.*, 31 F.4th 898, 903 (4th Cir. 2022) (no misrepresentation when Marriott made no representation about the "quality of its cybersecurity" practices); *In re Intel Corp. Sec. Litig.*, 2019 WL 1427660, at *9 (N.D. Cal. Mar. 29, 2019) (no liability for marketing statements with "vague positive statements" regarding security practices); *In re Heartland Payments Sys., Inc. Sec. Litig.*, 2009 WL 4798148, at *5-6 (D.N.J. Dec. 7, 2009) (no liability when allegations premised upon fact of the breach). In contrast, here, there are specific, affirmative statements about the "quality" of SolarWinds' cybersecurity practices. *See In re SolarWinds Corp.*, 595 F. Supp. 3d at 588 (distinguishing *Heartland* due to allegations of misrepresentations of SolarWinds' security practices); *In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d 1189, 1220-21 (N.D. Ga. 2019) (distinguishing *Heartland* due to misleading security statements).

V. Defendants Are Not Entitled to Summary Judgment on Mental State.

A. A Jury Should Decide Whether Defendants Acted With Scienter.

Defendants' attempt to move for summary judgment on scienter grounds on this mixed record is ill-fated. "Alleged absence of scienter is rarely an appropriate basis for granting summary judgment." *SEC v. DeFrancesco*, 699 F. Supp. 3d 228, 242 (S.D.N.Y. 2023) (citing *Press v. Chem. Inv. Servs. Corp.*, 166 F.3d 529, 538 (2d Cir. 1999)); *see also Terraform*, 708 F. Supp. 3d at 482 ("[w]hether to credit the SEC's interpretation or defendants' interpretation of the statements at issue…is a question for a jury, not for the Court."); *SEC v. Univ. Express, Inc.*, 475 F. Supp. 2d 412, 433-34 (S.D.N.Y. 2007), *aff'd sub nom. SEC v. Altomare*, 300 F. App'x 70 (2d Cir. 2008) (denying both parties' motions for summary judgment because "issues of fact remain as to…[Defendant's] state of mind at the time of his alleged conduct.").

Defendants next contend that to defeat summary judgment, the SEC's scienter evidence "must pertain to the risk of ***misleading investors***, not merely the risk that statements were false." [Def. Br. at 42-43 (emphasis in original)]. Defendants' argument misconstrues the law. The SEC is ***not*** required to show that Brown thought about investors in connection with the Security Statement. In the Second Circuit, the SEC may establish scienter "through a showing of reckless disregard for the truth, that is, conduct which is highly unreasonable and which represents an extreme departure from the standards of ordinary care." *SEC v. Obus*, 693 F.3d 276, 286 (2d Cir. 2012) (quoting *SEC v. McNulty*, 137 F.3d 732, 741 (2d Cir. 1998)). In sum, "[r]epresenting information as true while knowing it is not, recklessly misstating information, or asserting an opinion on grounds so flimsy as to belie any genuine belief in its truth, are all circumstances sufficient to support a conclusion of scienter." *Univ. Express*, 475 F. Supp. 2d at 424 (citation omitted); *see also SEC v. Constantin*, 939 F. Supp. 2d 288, 308 (S.D.N.Y. 2013).

This Court may infer scienter from circumstantial evidence where Defendants had knowledge of facts or access to information contradicting their public statements. *See SolarWinds Corp*., 741 F. Supp. 3d at 85 (holding that the SEC's Amended Complaint "easily pleads Brown's scienter" because "[i]t pleads that he approved the Security Statement and…was privy to internal information contradicting the Statement's representations both as to the company's access controls and compliance with the password policy."); *Novak v. Kasaks*, 216 F.3d 300, 308 (2d Cir. 2000). The record demonstrates numerous instances in which the Security Statement diverged from the facts as Brown knew them to be at the time, including relating to SolarWinds': (1) NIST Cybersecurity Framework compliance, *see* JS ¶¶67-69, 157, 163, 177, 179; SEC 56.1 ¶¶230-31, 234-37, 247-56; (2) access control policies, *see* JS ¶¶161, 164-165, 170, 172-177, 179-180, 184; SEC 56.1 ¶¶19, 30-31, 47, 49, 55-60, 64, 67-69, 91-92, 102-105, 109-111, 124-131, 133-134; (3) password policies, *see* JS ¶¶185, 187, 189; SEC 56.1 ¶¶161-68, 171-75; and (4) SDL policies, *see* JS ¶¶174-176, 191, 194, 199; SEC 56.1 ¶¶196-97, 202. "Brown's scienter is also properly imputed to SolarWinds." *SolarWinds Corp.*, 741 F. Supp. 3d at 86-87 (collecting cases); *see also In re Glob. Crossing, Ltd. Sec. Litig.*, 322 F. Supp. 2d 319, 336, 344 (S.D.N.Y. 2004). Thus, there are genuine issues of material fact about scienter.

Defendants next argue that the SEC cannot establish scienter because "Brown did not even write the Security Statement." [Def. Br. at 44]. Defendants' argument is foreclosed by the Parties' Joint Statement of Undisputed Facts, which acknowledged that "Mr. Brown, Ms. Johnson and Mr. Kim were all makers of the Security Statement for purposes of *Janus Capital Group, Inc. v. First Derivative Traders*, 564 U.S. 135 (2011)." [JS ¶35; *see also* SEC 56.1 ¶¶11-13]. The Supreme Court held in *Janus* that the "maker" of a statement for purposes of Rule 10b-5 "is the person or entity with ultimate authority over the statement, including its content and

whether and how to communicate it." *Janus*, 564 U.S. at 142. Thus, Brown was ultimately responsible for the content of the Security Statement and, as discussed above, there is evidence that he knew SolarWinds' actual cybersecurity practices diverged from the representations in the Security Statement, which is sufficient to establish a material dispute of fact as to scienter. *See id.; Univ. Express*, 475 F. Supp. 2d at 424; *see also Constantin*, 939 F. Supp. 2d at 308.

B. There Are Genuine Disputes of Material Fact as to Whether Defendants Acted With Negligence.

The elements of the SEC's Securities Act Section 17(a) claim are largely similar to the elements of the SEC's Section 10(b) claim, with one exception relevant here: Section 17(a)(2) and (3) only require proof of negligence, not scienter. *See Ginder*, 752 F.3d at 574. Under 17(a)(2) and (3), "the definition of negligence is the failure to use reasonable care, which is the degree of care that a reasonably careful person would use under like circumstances." *SEC v. Cole*, 2015 WL 5737275, at *6 (S.D.N.Y. Sept. 19, 2015) (cleaned up). As the *Cole* court held, "negligence is typically a jury determination." *Id.* at *6 (cleaned up). For the same reasons that there are genuine disputes of material fact as to whether Defendants acted with scienter, there are genuine disputes of material fact regarding whether Defendants acted with negligence. *See id.*

VI. SolarWinds' and Brown's Misstatements and Omissions Were Made "In Connection With" the Purchase or Sale of Securities.

Defendants misapprehend the broad scope of the securities laws when they claim the SEC cannot connect their fraud with a security transaction. [Def. Br. at 48]. Contrary to Defendants' suggestion, "the 'in connection with' factor has been broadly construed.… Any statement that is reasonably calculated to influence the average investor satisfies the 'in connection with' requirement of Rule 10b-5." *SEC v. Simeo*, 2021 WL 4041562, at *10 (S.D.N.Y. Sept. 3, 2021) (cleaned up). "Applying this standard, courts have concluded that publicly-disseminated press releases, research reports, and website representations that contain materially false and

misleading statements regarding an issuer of securities satisfies the 'in connection with' requirement." *SEC v. StratoComm Corp.*, 2 F. Supp. 3d 240, 258 (N.D.N.Y. 2014) (finding liability against defendant who made public statements that "falsely portrayed it as a development-stage company that had progressed to the operational stage with a finished product and sales, when it had not.") (collecting cases), *aff'd* 652 F. App'x 35 (2d Cir. 2016). The Court has already ruled with respect to Defendants' argument "that the Security Statement cannot be actionable because it was directed to *customers*, not investors" and held "[t]hat is wrong." *SolarWinds Corp.*, 741 F. Supp. 3d at 79 (emphasis in original). As the Court recognized, the Security Statement "was, unavoidably, part of the 'total mix of information' that SolarWinds furnished the investing public." *Id.* (quoting *Basic Inc.*, 485 U.S. at 232).

A court in this district found that a similar argument that a defendant's conduct did not occur "in the offer or sale of any securities," was "meritless" and "warrants limited discussion." *SEC v. Cole*, 2015 WL 5737275, at *7 (S.D.N.Y. Sept. 19, 2015). This is because "the Supreme Court has explained that 'Congress expressly intended to define these statutory terms broadly' and that these terms 'are expansive enough to encompass the entire selling process.'" *Id.* (quoting *United States v. Naftalin*, 441 U.S. 768, 773 (1979)). Here, SolarWinds executed a public offering on October 18, 2018, conducted a secondary public offering in May 2019, and offered employee stock purchase plans throughout the relevant period. [JS ¶2; SEC 56.1 ¶4].

Defendants seek to avoid the obvious connection to securities transactions here by relying on inapposite cases. [*See* Def. Br. at 48-50]. They cite to cases finding no such connection where:

- an executor allegedly defrauded an estate, *see D'Addario v. D'Addario*, 75 F.4th 86, 96 (2d Cir. 2023);
- "a defendant [sold] securities and then, at some later date, decide[d] to use the proceeds to cover-up an unrelated fraud," *SEC v. Morgan*, 2019 WL 2385395, at *8 (W.D.N.Y. June 5, 2019);

- it was not established that the defendant knew or should have known that certain emails would reach investors, *SEC v. Mahabub*, 343 F. Supp. 3d 1022, 1049 (D. Colo. 2018), *aff'd sub nom*. *SEC v. GenAudio Inc.*, 32 F.4th 902 (10th Cir. 2022);

- a wholly owned subsidiary "was not selling stock" and could not be held to have issued press releases in connection with a securities transaction, *Lindblom v. Mobile Telecommunications Techs. Corp.*, 985 F. Supp. 161, 164 (D.D.C. 1997).[13]

Defendants' fraudulent activities were undoubtedly in connection with a securities transaction and their arguments to the contrary should be rejected.

CONCLUSION

In light of the foregoing and for all of the reasons stated above, the Court should deny Defendants' Motion for Summary Judgment in its entirety.

June 13, 2025

Respectfully Submitted,

/s/ Christopher M. Bruckmann

Christopher M. Bruckmann
Christopher J. Carney
Kristen M. Warden (admitted *pro hac vice*)
John J. Todor (admitted *pro hac vice*)
William B. Ney (admitted *pro hac vice*)
Benjamin Brutlag
Lory Stone (admitted *pro hac vice*)
Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549
202-551-5986 (Bruckmann)
202-551-2379 (Carney)
202-551-4661 (Warden)
202-551-5381 (Todor)

[13] Although Defendants acknowledge that the SEC need not show reliance by investors as an element, Def. Br. 48, n. 42, they nonetheless point to an out-of-Circuit case where the court held that investors were not shown to have relied on the misstatements. *See Howard v. Arconic Inc.,* 395 F. Supp. 3d 516, 540 (W.D. Pa. 2019). They also cite to a case from another court in this District, in which the court parsed between statements it deemed "in connection" and those that were not, despite the "substance of the statements" being described as "similar." *See Hemming v. Alfin Fragrances, Inc.*, 690 F. Supp. 239, 245 (S.D.N.Y. 1988). That case is factually distinguishable and predates significant Supreme Court and Second Circuit precedent.

202-551-5317 (Ney)
202-551-2421 (Brutlag)
202-551-4931 (Stone)
BruckmannC@sec.gov
CarneyC@sec.gov
WardenK@sec.gov
TodorJ@sec.gov
NeyW@sec.gov
BrutlagB@sec.gov
StoneL@sec.gov

Attorneys for Plaintiff
Securities and Exchange Commission

CERTIFICATE OF SERVICE

I hereby certify that on June 13, 2025, I electronically filed the foregoing document with the Court via CM/ECF, which will automatically send notice and a copy of same to counsel of record via email.

/s/ Christopher M. Bruckmann
Christopher M. Bruckmann